AXIS A1601 Network Door Controller

Manual del usuario

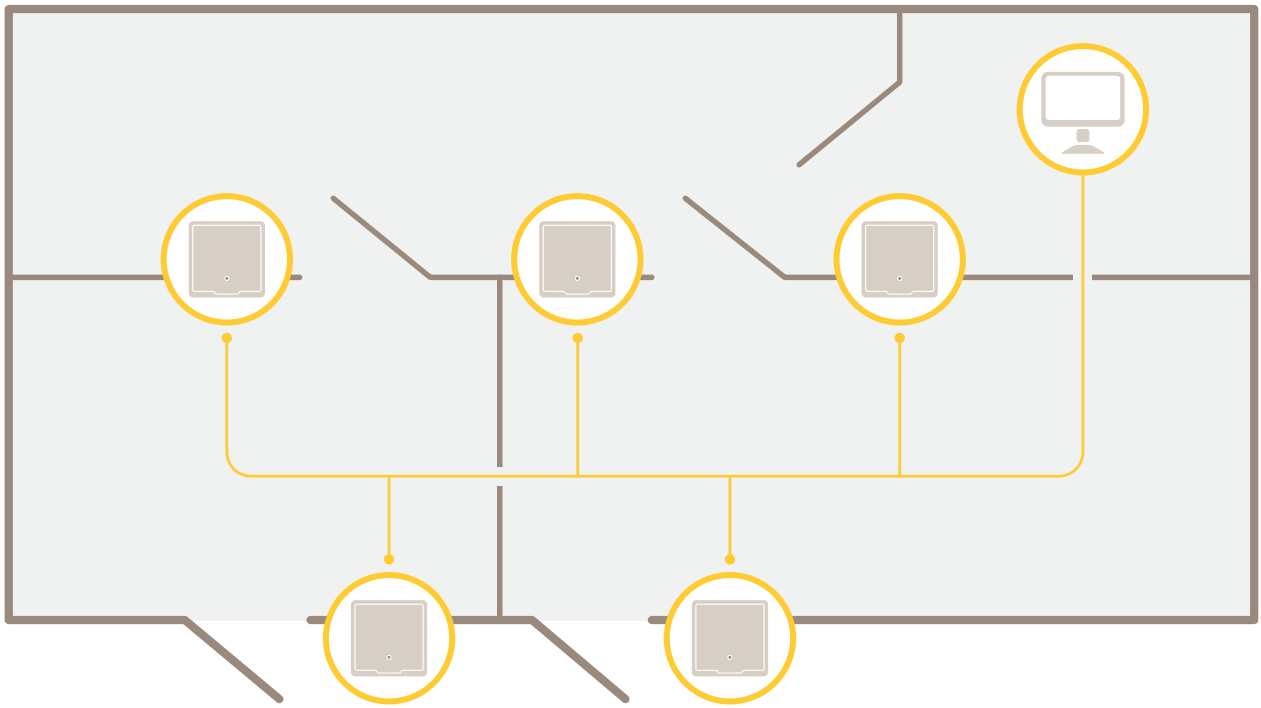
Índice

Presentación esquemática de la solución 5
Guía de productos 6
Localice el dispositivo en la red 7
Acceder al dispositivo 7
Cómo acceder al producto desde Internet 7
Contraseñas seguras 7
Cómo establecer la contraseña root 8
La página de Vista general 8
Configuración del sistema 9
Configuración: paso a paso 9
Seleccionar un idioma 9
Configurar fecha y hora 9
Obtener la fecha y hora desde un servidor Network Time Protocol (NTP). 10
Establecer la fecha y hora manualmente 10
Obtener la fecha y hora desde el ordenador 10
Configurar los ajustes de red 10
Configuración del hardware 11
Cómo importar un archivo de configuración de hardware 11
Crear una nueva configuración de hardware 12
Cómo crear una nueva configuración de hardware sin periféricos 12
Cómo crear una nueva configuración de hardware para cierres inalámbricos 15
Cómo crear una nueva configuración de hardware con control de ascensor (AXIS A9188) 16
Cómo añadir y configurar periféricos de red 16
Verifique las conexiones de hardware 17
Verificación de controles de puertas 17
Verificación de controles de plantas 18
Configure tarjetas y formatos 18
Descripciones de formatos de tarjeta 19
Formato de tarjeta 19
Mapas de campo 19
Configurar servicios 20
SmartIntego 21
Perfil LED OSDP 22
Instrucciones de mantenimiento 23
Configuración de eventos 24
Ver el registro de eventos 24
Filtros de registro de eventos 24
Configurar el registro de eventos 24
Opciones del registro de eventos 24
Cómo configurar reglas de acción 24
Cómo añadir destinatarios 25
Cómo crear programaciones 26
Cómo configurar repeticiones 26
Información del lector 27
Opciones del sistema 28
Seguridad 28
Usuarios 28
ONVIF 28
Filtro de direcciones IP 28
HTTPS 28
IEEE 802.1X 29
Certificados 29
Red 30

Ajustes básicos de TCP/IP 30
Advanced TCP/IP Settings 31
SOCKS 34
Calidad de Servicio (QoS) 34
SNMP 34
UPnP 35
Bonjour 35
Puertos y dispositivos 35
Puertos de E/S 35
Estado de puerto 35
Maintenance (Mantenimiento): 35
Asistencia técnica 36
Soporte de vista general 36
Descripción del sistema 36
Registros e informes 36
Avanzada 37
Secuencias de comandos 37
Carga de archivos 37
Localización de problemas 38
Restablezca la configuración predeterminada de fábrica 38
Cómo comprobar el firmware actual 38
Cómo actualizar el firmware 38
Síntomas, posibles causas y soluciones 39
Especificaciones 41
..... 41
Indicadores LED 41
Botones 41
Botón de control 41
Conectores 41
Conector de red 41
Conector de lector 42
Conector de puerta 43
Conector de relé 44
Conector auxiliar 45
Conector externo 46
Conector de alimentación 46
Conector de entrada de batería de reserva 46
Información de seguridad 48
Niveles de peligro 48
Otros niveles de mensaje 48
Interfaz web 49
..... 49
Estado 49
Dispositivo 50
Alarmas 50
Periféricos 51
Lectores 51
Cerraduras inalámbricas 52
Actualizar 52
Sistema 52
Hora y ubicación 52
Red 54
Seguridad 58
Cuentas 63
MQTT 64
Accesorios 67

Registros 67
Maintenance (Mantenimiento): 70

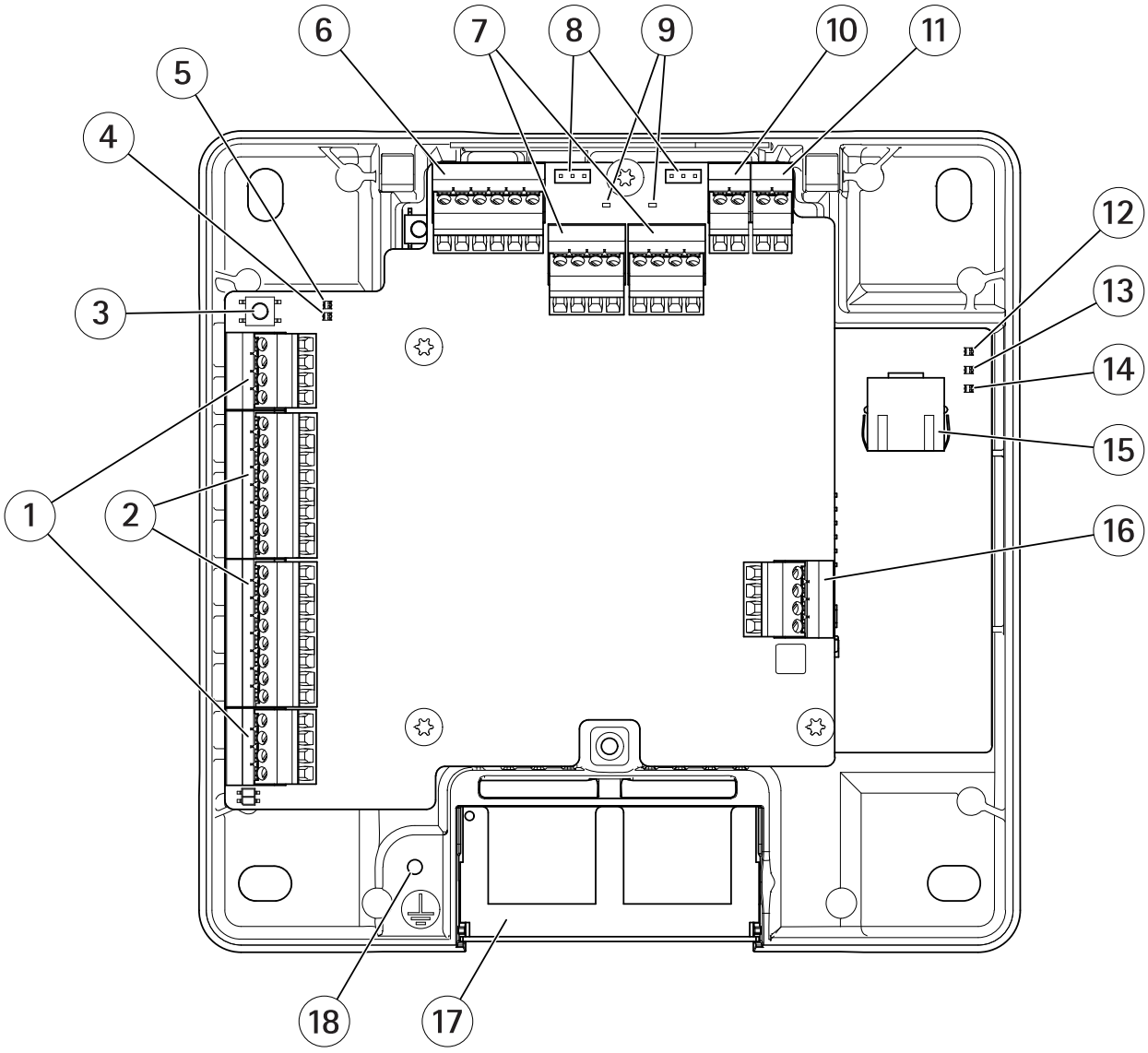
Presentación esquemática de la solución



El controlador de puerta en red se puede conectar fácilmente y recibirá alimentación de su red IP ya existente sin necesidad de cableado especial.

Cada controlador de puerta en red es un dispositivo inteligente fácil de montar junto a una puerta. Puede proporcionar alimentación y controlar hasta cuatro lectores.

Guía de productos



1 *Conector de puerta, on page 43 (2x)*
2 *Conector de lector, on page 42 (2x)*
3 *Botón de control, on page 41*
4 *LED de sobrecorriente de lector*
5 *Led de sobrecorriente del relé*
6 *Conector auxiliar, on page 45*
7 *Conector de relé, on page 44 (2x)*
8 *Puente de relé (2x)*
9 *LED de relé (2x)*
10 *Conector de entrada de batería de reserva, on page 46*
11 *Conector de alimentación, on page 46*
12 *LED de alimentación*
13 *LED de estado*
14 *LED de red*
15 *Conector de red, on page 41*
16 *Conector externo, on page 46*
17 *Cubierta de cable reversible*
18 *Posición de toma de tierra*

Localice el dispositivo en la red

Para localizar dispositivos de Axis en la red y asignarles direcciones IP en Windows®, utilice AXIS IP Utility o AXIS Device Manager. Ambas aplicaciones son gratuitas y pueden descargarse desde *axis.com/support*.

Para obtener más información acerca de cómo encontrar y asignar direcciones IP, vaya a *How to assign an IP address and access your device (Cómo asignar una dirección IP y acceder al dispositivo)*.

Acceder al dispositivo

1. Abra un navegador y escriba la dirección IP o el nombre de host del dispositivo Axis.
   Si no conoce la dirección IP, use AXIS IP Utility o AXIS Device Manager para localizar el dispositivo en la red.
2. Introduzca el nombre de usuario y la contraseña. Si accede al dispositivo por primera vez, debe establecer la contraseña root. Consulte .
3. Se abrirá la página web del dispositivo en el navegador. La página de inicio se denomina Overview (Descripción general).

Cómo acceder al producto desde Internet

Un router de red permite a los productos de una red privada (LAN) compartir una única conexión a Internet. Para ello, se transfiere el tráfico de red de la red privada a Internet.

La mayoría de los routers está preconfigurada para detener los intentos de acceso a la red privada (LAN) desde la red pública (Internet).

Si el producto de Axis se encuentra en una intranet (LAN) y quiere que esté disponible desde fuera (WAN) con un router NAT (Traducción de direcciones de red), active la **NAT transversal**. Con la NAT transversal configurada correctamente, se envía al producto todo el tráfico HTTP a un puerto externo HTTP en el router NAT.

Cómo activar la función de NAT transversal

- Vaya a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración del controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**.
- Haga clic en **Enable (Activar)**.
- Configure manualmente su router NAT para permitir el acceso desde Internet.

Nota

- En este contexto, un "router" hace referencia a cualquier dispositivo de enrutamiento de red, como un router NAT, un router de red, una puerta de enlace de Internet, un router de banda ancha, un dispositivo de uso compartido de banda ancha o un software, como un cortafuegos.
- Para que funcione la NAT transversal, debe ser compatible con el router. El router debe ser compatible también con UPnP®.

Contraseñas seguras

Importante

Utilice HTTPS (habilitado por defecto) para establecer su contraseña u otras configuraciones confidenciales a través de la red. El protocolo HTTPS habilita conexiones a la red seguras y cifradas, protegiendo así los datos confidenciales, como las contraseñas.

La contraseña del dispositivo es la principal protección para sus datos y servicios. Los dispositivos de Axis no imponen una política de contraseñas ya que pueden utilizarse en distintos tipos de instalaciones.

Para proteger sus datos le recomendamos encarecidamente que:

- Utilice una contraseña con al menos 8 caracteres, creada preferiblemente con un generador de contraseñas.

- No exponga la contraseña.
- Cambie la contraseña a intervalos periódicos y al menos una vez al año.

Cómo establecer la contraseña root

Para acceder al producto Axis, deberá establecer la contraseña para el administrador **root** predeterminado. Esta acción se lleva a cabo en el cuadro de diálogo **Configure Root Password (Configurar contraseña de root)**, que se abre cuando se accede al producto por primera vez.

Para evitar escuchas ilegales en la red, la contraseña de root se puede definir mediante una conexión HTTPS cifrada, que requiere un certificado HTTPS. HTTPS (protocolo de transferencia de hipertexto sobre SSL) es un protocolo que se usa para cifrar el tráfico entre los navegadores web y los servidores. El certificado HTTPS asegura el intercambio cifrado de información. Consulte *HTTPS, on page 28*.

El nombre de usuario administrador **root** predeterminado es permanente; no puede eliminarse. Si pierde la contraseña root, deberá restablecer el producto a los valores iniciales. Consulte *Restablezca la configuración predeterminada de fábrica, on page 38*.

Para definir la contraseña, escríbala directamente en el cuadro de diálogo.

La página de Vista general

La página de vista general en la página web del producto muestra información sobre el nombre, la dirección MAC, la dirección IP y la versión de firmware del controlador de puerta. También permite identificar el controlador de puerta en la red.

La primera vez que acceda al producto Axis, la página de vista general le pedirá que configure el hardware, establezca la fecha y hora y configure los ajustes de red. Para obtener más información acerca de cómo configurar el sistema, consulte *Configuración: paso a paso, on page 9*.

Para regresar a la página de vista general desde otras páginas web del producto, haga clic en **Overview (Vista general)** en la barra de menú.

Configuración del sistema

Para abrir las páginas de configuración del producto, haga clic en **Setup (Configuración)** en la esquina superior derecha de la página de vista general.

El producto de Axis puede ser configurado por administradores. Para obtener más información sobre usuarios y administradores, consulte *page 28*.

Configuración: paso a paso

Antes de empezar a utilizar el sistema de control de acceso, se deben completar los siguientes pasos de configuración:

1. Si el inglés no es su primera lengua, puede que prefiera que la página web del producto se muestre en un idioma diferente. Consulte *Seleccionar un idioma, on page 9*.
2. Configure la fecha y hora. Consulte *page 9*.
3. Configure los ajustes de red. Consulte *page 10*.
4. Configure el controlador de puerta y los dispositivos conectados, como lectores, cerraduras y dispositivos de solicitud de salida (REX). Consulte *Configuración del hardware, on page 11*.
5. Verifique las conexiones de hardware. Consulte *page 17*.
6. Configure tarjetas y formatos. Consulte *page 18*.

Para obtener información sobre las recomendaciones de mantenimiento, consulte *Instrucciones de mantenimiento, on page 23*.

Seleccionar un idioma

El idioma predeterminado de la página web del producto es inglés, pero puede cambiar a cualquiera de los idiomas incluidos en el firmware del producto. Para obtener información sobre el firmware más reciente disponible, consulte *www.axis.com*

Se puede cambiar el idioma en cualquiera de las páginas web del producto.

Para cambiar de idioma, haga clic en la lista desplegable de idioma y seleccione un idioma. Todas las páginas web y páginas de ayuda del producto se muestran en el idioma seleccionado.

Nota

- Cuando se cambia el idioma, también cambia el formato de fecha en un formato utilizado habitualmente en el idioma seleccionado. El formato correcto se muestra en los campos de datos.
- Si se restablecen los ajustes predeterminados de fábrica, la página web del producto se vuelve a mostrar en inglés.
- Si se restaura o se reinicia el producto o se actualiza el firmware, la página web del producto se seguirá mostrando en el idioma seleccionado.

Configurar fecha y hora

Para configurar la fecha y hora del producto Axis, vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.

Puede definir la fecha y hora de las formas siguientes:

- Obtener la fecha y hora de un servidor Network Time Protocol (NTP). Consulte *page 10*.
- Establecer la fecha y hora manualmente. Consulte *page 10*.
- Obtener la fecha y hora del ordenador. Consulte *page 10*.

Current controller time (Hora actual del controlador) muestra la fecha y hora actual del controlador de puerta (reloj de 24 horas).

Las mismas opciones de fecha y hora también están disponibles en las páginas de opciones del sistema. Vaya a **Setup (Configuración)> Additional Controller Configuration (Configuración de controlador adicional)> System Options (Opciones del sistema) > Date & Time (Fecha y hora)**.

Obtener la fecha y hora desde un servidor Network Time Protocol (NTP).

1. Vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.
2. Seleccione su **Timezone (Zona horaria)** en la lista desplegable.
3. Si se utiliza horario de verano en su región, seleccione **Adjust for daylight saving (Ajustar para horario de verano)**.
4. Seleccione **Synchronize with NTP (Sincronizar con NTP)**.
5. Seleccione la dirección DHCP predeterminada o introduzca la dirección de un servidor NTP.
6. Haga clic en **Save (Guardar)**.

Al sincronizar con un servidor NTP, la fecha y la hora se actualizan continuamente porque los datos se insertan desde el servidor NTP. Para obtener información sobre los ajustes de NTP, consulte *Configuración de NTP, on page 32*.
Si se utiliza un nombre de host para el servidor NTP, se debe configurar un servidor DNS. Consulte *Configuración de DNS, on page 31*.

Establecer la fecha y hora manualmente

1. Vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.
2. Si se utiliza horario de verano en su región, seleccione **Adjust for daylight saving (Ajustar para horario de verano)**.
3. Seleccione **Set date & time manually (Establecer fecha y hora manualmente)**.
4. Introduzca manualmente la fecha y la hora deseadas.
5. Haga clic en **Save (Guardar)**.

Al definir la fecha y la hora manualmente, estas se establecen una única vez sin posteriores actualizaciones automáticas. Esto significa que, si se deben actualizar la fecha o la hora, los cambios se deben realizar manualmente porque no hay conexión con un servidor NTP externo.

Obtener la fecha y hora desde el ordenador

1. Vaya a **Setup > Date & Time (Configuración > Fecha y hora)**.
2. Si se utiliza horario de verano en su región, seleccione **Adjust for daylight saving (Ajustar para horario de verano)**.
3. Seleccione **Set date & time manually (Establecer fecha y hora manualmente)**.
4. Haga clic en **Sync now and save (Sincronizar ahora y guardar)**.

Cuando se utiliza la hora del ordenador, la fecha y hora se sincronizan con la fecha y hora del ordenador una única vez, sin actualizaciones automáticas posteriores. Esto significa que si se cambia la fecha y hora en el equipo que utilice para gestionar el sistema, debe sincronizar nuevo.

Configurar los ajustes de red

Para configurar los ajustes básicos de red, vaya a **Setup > Network Settings (Configuración > Ajustes de red)** o a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Básica)**.

Para obtener más información sobre los ajustes de red, consulte *Red, on page 30*.

Configuración del hardware

Puede conectar lectores, cerraduras y otros dispositivos al producto de Axis antes de finalizar la configuración del hardware. Sin embargo, la conexión de dispositivos será más fácil si completa la configuración de hardware primero. Esto se debe a que un gráfico de pines del hardware estará disponible cuando la configuración esté completa. El gráfico de pines del hardware es una guía sobre cómo conectar los dispositivos a los pines. Se puede usar como hoja de referencia para tareas de mantenimiento. Para consultar las instruccionesde mantenimiento, vea *page 23*.

Para configurar el hardware por primera vez, seleccione uno de los siguientes métodos:

- Importación de un archivo de configuración de hardware. Consulte *page 11*.
- Crear una nueva configuración de hardware. Consulte *page 12*.

Nota

Si el hardware del producto no se ha configurado antes o se ha eliminado, **Hardware Configuration (Configuración de hardware)** estará disponible en el panel de notificación de la página Overview (Descripción general).

Cómo importar un archivo de configuración de hardware

La configuración del hardware del producto de Axis se puede completar más rápidamente mediante la importación de un archivo de configuración de hardware.

Al exportar el archivo desde un producto e importarlo en otros, se pueden hacer numerosas copias de la misma configuración de hardware sin tener que repetir los mismos pasos una y otra vez. También se pueden almacenar los archivos exportados como copias de seguridad y usarlos para restaurar configuraciones de hardware previas. Para obtener más información, consulte *Cómo exportar un archivo de configuración de hardware, on page 11*.

Para importar un archivo de configuración de hardware:

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)**.
2. Haga clic en **Import hardware configuration (Importar configuración de hardware)**. Si ya existe una configuración de hardware, haga clic en **Reset and import hardware configuration (Restablecer e importar una configuración de hardware)**.
3. En el cuadro de diálogo del navegador de archivos que aparece, localice y seleccione el archivo de configuración de hardware (*.json) en su equipo.
4. Haga clic en **OK**.

Cómo exportar un archivo de configuración de hardware

La configuración de hardware del producto de Axis se puede exportar para realizar múltiples copias de la misma configuración de hardware. También se pueden almacenar los archivos exportados como copias de seguridad y usarlos para restaurar configuraciones de hardware previas.

Nota

No es posible exportar la configuración de hardware de plantas.

La configuración de las cerraduras inalámbricas no se incluye en la exportación de la configuración de hardware.

Para exportar un archivo de configuración de hardware:

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)**.
2. Haga clic en **Export hardware configuration (Exportar configuración de hardware)**.
3. En función del navegador, es posible que se muestre un cuadro de diálogo para completar la exportación.
   A menos que se especifique lo contrario, el archivo exportado (*.json) se guarda en la carpeta de descargas predeterminada. Se puede seleccionar una carpeta de descargas en la configuración de usuario del navegador web.

Crear una nueva configuración de hardware

Siga las instrucciones de acuerdo con sus necesidades:

- *Cómo crear una nueva configuración de hardware sin periféricos, on page 12*
- *Cómo crear una nueva configuración de hardware para cierres inalámbricos, on page 15*
- *Cómo crear una nueva configuración de hardware con control de ascensor (AXIS A9188), on page 16*

Cómo crear una nueva configuración de hardware sin periféricos

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)** y haga clic en **Start new hardware configuration (Iniciar nueva configuración de hardware)**.
2. Introduzca el nombre del producto Axis.
3. Seleccione el número de puertas conectadas y haga clic en **Next (Siguiente)**.
4. Configure los monitores de puerta (sensores de posición de puerta) y las cerraduras según sus necesidades y haga clic en **Next (Siguiente)**. Para obtener más información sobre las opciones disponibles, consulte *Cómo configurar monitores y cerraduras de puerta, on page 12*.
5. Configure los lectores y dispositivos REX que se utilizarán y haga clic en **Finish (Finalizar)**. Para obtener más información sobre las opciones disponibles, consulte *Cómo configurar lectores y dispositivos REX, on page 14*.
6. Haga clic en **Close (Cerrar)** o en el enlace para ver el gráfico de pines del hardware.

Cómo configurar monitores y cerraduras de puerta

Si se selecciona una opción de puerta en la nueva configuración de hardware, puede configurar los monitores de puerta y cerraduras.

1. Si se utilizará un monitor de puerta, seleccione **Door Monitor (Monitor de puerta)** y, a continuación, seleccione la opción que coincida con el modo en que se conectarán los circuitos del monitor de puerta.
2. Si la cerradura de puerta debe bloquearse inmediatamente después de abrirse la puerta, seleccione **Cancel access time once door is opened (Cancelar tiempo de acceso una vez abierta la puerta)**.
   Si desea retrasar el bloqueo, defina el tiempo de retraso en milisegundos en **Relock time (Tiempo para bloqueo)**.
3. Especifique las opciones de tiempo del monitor de puerta o, si no se utilizará ningún monitor de puerta, las opciones de tiempo de bloqueo.
4. Seleccione las opciones que se ajusten al modo en que se conectarán los circuitos de la cerradura.
5. Si se utilizará un monitor de cerradura, seleccione **Lock Monitor (Monitor de cerradura)** y, a continuación, seleccione las opciones que coincidan con el modo en que se conectarán los circuitos del monitor de cerradura.
6. Si se deben supervisar las conexiones de entrada procedentes de lectores, dispositivos REX y monitores de puerta, seleccione **Enable supervised inputs (Habilitar entradas supervisadas)**.
   Para obtener más información, consulte *Cómo usar entradas supervisadas, on page 15*.

Nota

- La mayoría de las opciones de cerradura, monitor de puerta y lector se pueden modificar sin restablecer e iniciar una nueva configuración de hardware. Vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de hardware)**.
- Puede conectar un único monitor de cerradura por controlador de puerta. De este modo, si lo que si utiliza puertas de cerradura doble, solo una de las cerraduras puede tener un monitor de cerradura. Si hay dos puertas conectadas al mismo controlador de puerta, no se pueden utilizar monitores de cerradura.

Acerca de las opciones de monitor de puerta y hora

Las siguientes opciones de monitor de puerta están disponibles:

- **Door monitor (Monitor de puerta)**: seleccionado por defecto. Cada puerta tiene su propio monitor de puerta que, por ejemplo, señalará si la puerta es forzada o permanece abierta durante un tiempo demasiado largo. Anule la selección si no se utilizará ningún monitor de puerta.

– **Open circuit = Closed door (Circuito abierto = Puerta cerrada)**: seleccione esta opción si el circuito del monitor de puerta está normalmente abierto. El monitor de puerta proporciona la señal de puerta abierta cuando el circuito está cerrado. El monitor de puerta proporciona la señal de puerta cerrada cuando el circuito está abierto.

– **Open circuit = Open door (Circuito abierto = Puerta abierta)**: seleccione esta opción si el circuito del monitor de puerta está normalmente cerrado. El monitor de puerta proporciona la señal de puerta abierta cuando el circuito está abierto. El monitor de puerta proporciona la señal de puerta cerrada cuando el circuito está cerrado.

- **Cancel access time once door is opened (Cancelar tiempo de acceso una vez que se abre la puerta)**: seleccione esta opción para prevenir infiltraciones. La cerradura se bloqueará tan pronto como el monitor de puerta señale que la puerta se ha abierto.

La siguientes opciones de tiempo de puerta están siempre disponibles:

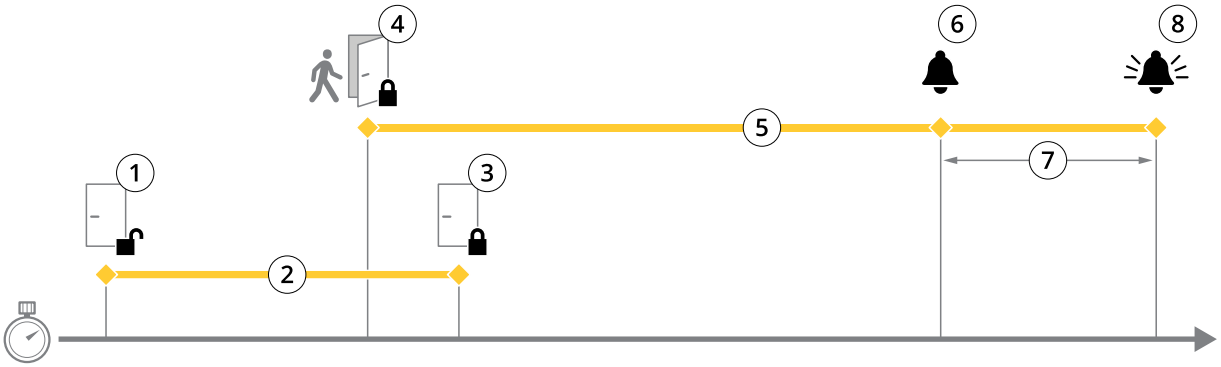
- **Access time (Tiempo de acceso)**: establece el número de segundos que la puerta permanecerá desbloqueada una vez se ha concedido permiso de acceso. La puerta permanecerá desbloqueada hasta que se abra o hasta que haya transcurrido el intervalo de tiempo establecido. La puerta se bloqueará una vez cerrada, independientemente de que el tiempo de acceso no haya expirado.

- **Long access time (Tiempo de acceso largo)**: establece el número de segundos que la puerta permanecerá desbloqueada una vez que se ha concedido permiso de acceso. El tiempo de acceso largo reemplaza el tiempo de acceso establecido y se activará para los usuarios en los que se haya seleccionado el tiempo de acceso largo.

Seleccione **Door monitor (Monitor de puerta)** para disponer de las siguientes opciones de tiempo de puerta:

- **Open too long time (Tiempo de apertura demasiado largo)**: establece el número de segundos que se permite que la puerta esté abierta. Si la puerta sigue abierta una vez transcurrido el período de tiempo determinado, se activa la alarma de puerta abierta durante demasiado tiempo. Configure una regla de acción para determinar qué acción debe activar el evento de puerta abierta durante demasiado tiempo.

- **Pre-alarm time (Tiempo de alarma previa)**: una alarma previa es una señal de advertencia que se activa antes de que se haya alcanzado el tiempo de apertura durante demasiado tiempo. Informa al administrador y advierte, en función de la configuración de la regla de acción, a la persona que entra por la puerta que esta debe cerrarse a fin de evitar que se active la alarma de puerta abierta durante demasiado tiempo. Defina el número de segundos durante el cual se dará la señal de advertencia previa a la alarma antes de que el sistema active la alarma de puerta abierta durante demasiado tiempo. Para deshabilitar la advertencia previa a la alarma, defina el tiempo previo a la alarma al valor 0.



1 Acceso concedido: desbloquea las cerraduras
2 Tiempo de acceso
3 Ninguna acción realizada: bloquea las cerraduras
4 Acción realizada (puerta abierta): bloquea las cerraduras o las mantiene desbloqueadas hasta que se cierre la puerta
5 Tiempo de apertura demasiado largo

6 *Se desactiva el tiempo previo a la alarma*
7 *Tiempo previo a la alarma*
8 *La alarma de tiempo de apertura demasiado largo se desactiva*

Para obtener información sobre cómo configurar una regla de acción, consulte *Cómo configurar reglas de acción, on page 24*.

Acerca de las opciones de cerradura

Las siguientes opciones de circuito de cerradura están disponibles:

- **Relay (Relé)**: solo se puede utilizar en una única cerradura por controlador de puerta. Si hay dos puertas conectadas al controlador de puerta, solamente se puede utilizar un relé en la cerradura de la segunda puerta.
- **Ninguno** – Solo disponible para el Bloqueo 2. Seleccione esta opción si solo se va a utilizar un bloqueo.

Las siguientes opciones de monitor de cerradura están disponibles para configuraciones de puerta única:

- **Lock monitor (Monitor de cerradura)**: seleccione esta opción para hacer disponibles los controles del monitor de cerradura. A continuación, seleccione la cerradura que se debe monitorizar. Solo se puede utilizar un monitor de cerradura en puertas de doble cerradura, pero no se puede utilizar si dos puertas están conectadas al controlador de puerta.

– **Open circuit = Locked (Circuito abierto = bloqueado)**: seleccione esta opción si el circuito de monitor de cerradura está normalmente cerrado. El monitor de cerradura proporciona la señal de desbloqueo de puerta cuando el circuito está cerrado. El monitor de cerradura proporciona a la puerta la señal de bloqueo cuando el circuito está abierto.

– **Open circuit = Unlocked (Circuito abierto = bloqueado)**: seleccione esta opción si el circuito de monitor de cerradura está normalmente abierto. El monitor de cerradura proporciona la señal de desbloqueo de puerta cuando el circuito está abierto. El monitor de cerradura proporciona a la puerta la señal de bloqueo cuando el circuito está cerrado.

Cómo configurar lectores y dispositivos REX

Una vez configurados los monitores de puerta y las cerraduras en la nueva configuración de hardware, puede configurar los lectores y dispositivos de solicitud de salida (REX).

1. Si se utilizará un lector, seleccione la casilla de verificación y, a continuación, seleccione las opciones que coincidan con el protocolo de comunicación del lector.
2. Si se utiliza un dispositivo REX, como un botón, un sensor o una barra de empuje, seleccione la casilla de verificación y, a continuación, seleccione la opción que coincida con el modo en que se conectarán los circuitos del dispositivo REX.
   Si la señal de REX no influye en la apertura de la puerta (por ejemplo, para puertas con manillas mecánicas o barras de empuje), seleccione **REX no desbloquea la puerta**.
3. Si se conecta más de un lector o un dispositivo REX al controlador de puerta, repita los dos pasos anteriores hasta que cada lector o dispositivo REX tenga la configuración correcta.

Acerca de las opciones de lector y dispositivo REX

Están disponibles las siguientes opciones de lector:

- **Wiegand**: seleccione esta opción para lectores que utilizan protocolos Wiegand. A continuación, seleccione el control de LED compatible con el lector. Por lo general, los lectores de un único control de LED alternan entre rojo y verde. Los lectores con control de led dual utilizan diferentes cables para los LED rojo y verde. Esto significa que los LED se controlan de manera independiente. Cuando se activan los dos LED, la luz se muestra ámbar. Consulte la información del fabricante en relación con el control de LED que admite el lector.
- **OSDP, half-duplex RS485**: seleccione esta opción para lectores RS485 que admiten half-duplex. Consulte la información del fabricante en relación con el protocolo que admite el lector.

Las siguientes opciones de dispositivo REX están disponibles:

- **Active low (Activar bajo)**: seleccione esta opción si el circuito se cierra al activarse el dispositivo REX.

- **Active high (Activar alto)**: seleccione esta opción si el dispositivo REX abre el circuito.
- **REX does not unlock door (REX no desbloquea la puerta)**: seleccione esta opción si la señal de REX no influye en la apertura de la puerta (por ejemplo, para puertas con manillas mecánicas o barras de empuje). La alarma de apertura forzada de puerta no se activará si el usuario abre la puerta dentro del tiempo de acceso. Anule la selección si la puerta se debe desbloquear automáticamente cuando el usuario activa el dispositivo REX.

Nota

La mayoría de las opciones de cerradura, monitor de puerta y lector se pueden modificar sin restablecer e iniciar una nueva configuración de hardware. Vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de hardware)**.

Cómo usar entradas supervisadas

Las entradas supervisadas informan acerca del estado de la conexión entre el controlador de puerta y los monitores de puerta. Si se interrumpe la conexión, se activa un evento.

Para utilizar entradas supervisadas:

1. Instale resistencias de final de línea en todas las entradas supervisadas. Consulte el diagrama de conexión en *page 43*.
2. Vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de hardware)** y seleccione **Enable supervised inputs (Habilitar entradas supervisadas)**. También puede habilitar las entradas supervisadas durante la configuración de hardware.

Acerca de la compatibilidad con la entrada supervisada

La función siguiente es compatible con entradas supervisadas:

- Monitor de puerta. Consulte *Conector de puerta, on page 43*.

Cómo crear una nueva configuración de hardware para cierres inalámbricos

1. Vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)** y haga clic en **Start new hardware configuration (Iniciar nueva configuración de hardware)**.
2. Introduzca el nombre del producto Axis.
3. En la lista de periféricos, seleccione un fabricante para la puerta de enlace inalámbrica.
4. Si quiere conectar una puerta con cable, seleccione la casilla **1 Door (1 puerta)** y haga clic en **Next (Siguiente)**. Si no se incluye ninguna puerta, haga clic en **Finish (Finalizar)**.
5. En función de su fabricante de cerraduras, continúe según uno de los puntos:
   - **ASSA Aperio**: Haga clic en el enlace para ver el gráfico de pines del hardware o haga clic en **Close (Cerrar)** y vaya a **Setup > Hardware Reconfiguration (Configuración > Reconfiguración de hardware)** para completar la configuración; consulte *Añadir puertas y dispositivos Assa Aperio™, on page 15*
   - **SmartIntego**: Haga clic en el enlace para ver el gráfico de pines del hardware o haga clic en **Click here to select wireless gateway and configure doors (Haga clic aquí para seleccionar la puerta de enlace inalámbrica y configurar puertas)** para completar la configuración; consulte *Cómo configurar SmartIntego, on page 21*.

Añadir puertas y dispositivos Assa Aperio™

Antes de añadir una puerta inalámbrica al sistema, es necesario emparejarse con el concentrador de comunicaciones Assa Aperio mediante la herramienta de aplicación de programación Aperio PAP.

Para añadir una puerta inalámbrica:

1. Acceda a **Setup (Configuración)** > **Hardware Reconfiguration (Reconfiguración de hardware)**.
2. Debajo de Wireless Doors and Devices (Puertas y dispositivos inalámbricos), haga clic en **Add door (Añadir puerta)**.

3. En el campo **Door name (Nombre de puerta)**: Introduzca un nombre descriptivo.
4. En el campo **ID (Identificación)**, debajo de **Lock (Cerradura)**: introduzca la dirección de seis caracteres del dispositivo que desee añadir. La dirección del dispositivo aparece impresa en la etiqueta del producto.
5. Si lo desea, en **Door position sensor (Sensor de posición de puerta externo)**: Seleccione **Built in door position sensor (Sensor de posición de puerta integrado)** o **External door position sensor (Sensor de posición de puerta externo)**.

Nota

Si utiliza un sensor de posición de puerta externo, asegúrese de que el dispositivo de bloqueo Aperio es compatible con la detección de estado del mango de la puerta antes de configurarlo.

6. Si lo desea, en el campo **ID** en **Door position sensor (Sensor de posición de puerta)**: introduzca la dirección de seis caracteres del dispositivo que desee añadir. La dirección del dispositivo aparece impresa en la etiqueta del producto.
7. Haga clic en **Add (Añadir)**.

Cómo crear una nueva configuración de hardware con control de ascensor (AXIS A9188)

Importante

Antes de crear una configuración de hardware, tiene que agregar un usuario a AXIS A9188 Network I/O Relay Module. Vaya a la interfaz web A9188> **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencias > Configuración del dispositivo adicional> Configuración básica> Usuarios> Agregar> Configuración de usuario)**.

Nota

Se puede configurar un máximo de 2 AXIS 9188 Network I/O Relay Module con cada Axis Network Door Controller

1. En la página web de controlador de puerta, vaya a **Setup > Hardware Configuration (Configuración > Configuración de hardware)** y haga clic en **Start new hardware configuration (Iniciar nueva configuración de hardware)**.
2. Introduzca el nombre del producto Axis.
3. En la lista de periféricos, seleccione **Elevator control (Control de ascensor)** para incluir AXIS A9188 Network I/O Relay Module y haga clic en **Next (Siguiente)**.
4. Introduzca el nombre del lector conectado.
5. Seleccione los protocolos de lectores que se utilizarán y haga clic en **Finish (Finalizar)**.
6. Haga clic en **Network Peripherals (Periféricos de red)** para completar la configuración. Consulte *Cómo añadir y configurar periféricos de red , on page 16* o haga clic en el enlace para acceder al gráfico de pines del hardware.

Cómo añadir y configurar periféricos de red

Importante

- Antes de configurar los periféricos de red, se debe añadir un usuario en AXIS A9188 Network I/O Relay Module. Vaya a la interfaz web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencias > Configuración del dispositivo adicional> Configuración básica> Usuarios> Agregar> Configuración de usuario)**.
- No añada otro AXIS A1001 Network Door Controller como periférico de red.

1. Vaya a **Setup > Network Periphals (Configuración > Periféricos de red)** para añadir un dispositivo
2. Identifique su dispositivo en **Dispositivos detectados**.
3. Haga clic en **Add this device (Añadir este dispositivo)**
4. Introduzca un nombre para el dispositivo
5. Introduzca el nombre de usuario y la contraseña para AXIS A9188.

6. Haga clic en **Add (Añadir)**.

Nota

Puede añadir manualmente periféricos de red introduciendo la dirección MAC o la dirección IP en el cuadro de diálogo **Manually add device (Añadir dispositivo manualmente)**.

Importante

Si quiere eliminar una programación, asegúrese primero de que el módulo de relé de E/S de red no la utiliza.

Cómo configurar E/S y relés de periféricos en red

Importante

Antes de configurar los periféricos de red, se debe añadir un usuario en AXIS A9188 Network I/O Relay Module. Vaya a la interfaz web AXIS A9188 > **Preferences > Additional device configuration > Basic setup > Users > Add > User setup (Preferencias > Configuración del dispositivo adicional> Configuración básica> Usuarios> Agregar> Configuración de usuario)**.

1. Vaya a **Setup > Network Periphals (Configuración > Periféricos de red)** y haga clic en la fila **Added devices (Dispositivos añadidos)**.
2. Seleccione los E/s y relés que se establecerán como planta.
3. Haga clic en **Set as floor (Establecer como planta)** e introduzca un nombre.
4. Haga clic en **Add (Añadir)**.

Verifique las conexiones de hardware

Una vez completada la instalación y la configuración de hardware, y en cualquier momento durante la vida útil del controlador de puerta, se puede verificar el funcionamiento de los monitores de puerta conectados, los módulos de relé de E/S de red, las cerraduras y los lectores.

Para verificar la configuración y el acceso a los controles de verificación, vaya a **Setup > Hardware Connection Verification (Configuración > Verificación de conexión de hardware)**.

Verificación de controles de puertas

- **Estado de puerta**: verificar el estado actual del monitor de puerta, alarmas de puerta y cerraduras. Haga clic en **Get current state (Obtener estado actual)**.
- **Cerradura**: activa manualmente la cerradura. Las cerraduras principales y secundarias, en su caso, se verán afectadas. Haga clic en **Lock (Bloquear)** o **Unlock (Desbloquear)**.
- **Lock (Cerradura)**: activa manualmente la cerradura para permitir el acceso. Solo se verán afectadas las cerraduras principales. Haga clic en **Access (Acceso)**.
- **Reader: Feedback (Lector: Respuesta)**: verifica la información del lector, como sonidos y señales LED, para distintos comandos. Seleccione el comando y haga clic en **Test (Prueba)**. Los tipos de información disponibles dependen del lector. Para obtener más información, consulte *Información del lector, on page 27*. Consulte también las instrucciones del fabricante.
- **Reader: Tampering (Lector: Manipulación)**: proporciona información sobre el último intento de manipulación. El primer intento de manipulación se registrará al instalar el lector. Haga clic en **Get last tampering (Obtener última manipulación)**.
- **Reader: Card swipe (Lector: Deslizar tarjeta)**: proporciona información sobre la última tarjeta leída u otros tipos de comprobante aceptados por el lector. Haga clic en **Get last credential (Obtener últimas credenciales)**.
- **REX**: proporciona información sobre la última vez que se pulsó el dispositivo de solicitud de salida (REX). Haga clic en **Get last REX (Obtener última REX)**.

Verificación de controles de plantas

- **Floor state (Estado de planta)**: verifica el estado actual de acceso a la planta. Haga clic en **Get current state (Obtener estado actual)**.
- **Floor lock & unlock (Bloquear y desbloquear planta)**: activa manualmente el acceso a la planta. Las cerraduras principales y secundarias, en su caso, se verán afectadas. Haga clic en **Lock (Bloquear)** o **Unlock (Desbloquear)**.
- **Floor access (Acceso a planta)**: concede manualmente acceso temporal a la planta. Solo se verán afectadas las cerraduras principales. Haga clic en **Access (Acceso)**.
- **Elevator Reader: Feedback (Lector elevador: Respuesta)**: verifica la información del lector, como sonidos y señales LED, para distintos comandos. Seleccione el comando y haga clic en **Test (Prueba)**. Los tipos de información disponibles dependen del lector. Para obtener más información, consulte *Información del lector, on page 27*. Consulte también las instrucciones del fabricante.
- **Elevator Reader: Tampering (Lector elevador: Manipulación)**: proporciona información sobre el último intento de manipulación. El primer intento de manipulación se registrará al instalar el lector. Haga clic en **Get last tampering (Obtener última manipulación)**.
- **Elevator Reader: Card swipe (Lector elevador: Deslizar tarjeta)**: proporciona información sobre la última tarjeta leída u otros tipos de comprobante aceptados por el lector. Haga clic en **Get last credential (Obtener últimas credenciales)**.
- **REX**: proporciona información sobre la última vez que se pulsó el dispositivo de solicitud de salida (REX). Haga clic en **Get last REX (Obtener última REX)**.

Configure tarjetas y formatos

El controlador de puerta incorpora algunos formatos de tarjeta predefinidos habitualmente utilizados que se pueden utilizar o modificar en función de las necesidades. También se pueden crear formatos de tarjeta personalizados. Cada formato de tarjeta incluye un conjunto de reglas y mapas de campo diferentes para la forma de organizar la información almacenada en la tarjeta. Al definir un formato de tarjeta, se indica al sistema cómo se debe interpretar la información que el controlador recibe del lector. Para obtener información acerca de los tipos de formato de tarjeta compatibles con el lector, consulte las instrucciones del fabricante.

Para habilitar formatos de tarjeta:

1. Vaya a **Setup > Configure cards and formats (Configuración > Configurar tarjetas y formatos)**.
2. Seleccione uno o varios formatos de tarjeta que coincidan con el formato de tarjeta utilizado por los lectores conectados.

Para crear nuevos formatos de tarjeta:

1. Vaya a **Setup > Configure cards and formats (Configuración > Configurar tarjetas y formatos)**.
2. Haga clic en **Add card format (Añadir formato de tarjeta)**.
3. En el cuadro de diálogo **Add card format (Añadir formato de tarjeta)**, introduzca el nombre, la descripción y la longitud de bits del formato de tarjeta. Consulte *Descripciones de formatos de tarjeta, on page 19*.
4. Haga clic en **Add field map (Añadir mapa de campo)** e introduzca la información requerida en los campos. Consulte *Mapas de campo, on page 19*.
5. Para añadir varios mapas de campo, repita el paso anterior.

Para expandir un elemento en la lista **Card formats (Formatos de tarjeta)** y ver las descripciones de formato de tarjeta y mapas de campo, haga clic en .

Para editar un formato de tarjeta, haga clic en ,255mm,sfx)=″graphics:graphic820C1116506B66D5D1FA49760B7A7266″ y modifique las descripciones de formato de tarjeta y mapas de campo de acuerdo con sus necesidades. A continuación, haga clic en **Save (Guardar)**.

Para eliminar un mapa de campo en el cuadro de diálogo **Edit card format (Editar formato de tarjeta)** o **Add card format (Añadir formato de tarjeta)**, haga clic en
,255mm,sfx)=″graphics:graphicDC3A5D4C4BA1B405B8634B9FB63D5327″

Para eliminar un formato de tarjeta, haga clic en
,255mm,sfx)=″graphics:graphicDC3A5D4C4BA1B405B8634B9FB63D5327″.

Importante

- Solo se pueden activar y desactivar formatos de tarjeta si el controlador de puerta se ha configurado con al menos un lector. Vea *Configuración del hardware, on page 11* y *Cómo configurar lectores y dispositivos REX, on page 14*.
- No pueden estar activos simultáneamente dos formatos de tarjeta con la misma longitud de bits. Por ejemplo, si se han definido dos formatos de tarjeta de 32 bits, "Formato A" y "Formato B", y se ha habilitado el "Formato A", no se puede habilitar el "Formato B" sin deshabilitar primero el "Formato B".
- Si no hay formatos de tarjeta habilitados, se pueden utilizar los tipos de identificación **Card raw only (Solo tarjeta sin formato)** y **Card raw and PIN (Tarjeta sin formato y PIN)** para identificar una tarjeta y permitir el acceso a los usuarios. Sin embargo, no se recomienda, dado que diferentes fabricantes o diferentes configuraciones de lectores pueden generar distintos datos de tarjeta sin formato.

Descripciones de formatos de tarjeta

- **Name (Nombre)** (obligatorio): introduzca un nombre descriptivo.
- **Description (Descripción)**: introduzca la información adicional que desee. Esta información solo es visible en los cuadros de diálogo **Edit card format (Editar formato de tarjeta)** y **Add card format (Añadir formato de tarjeta)**.
- **Bit length (Longitud de bits)** (obligatorio): escriba la longitud de bits del formato de tarjeta. Debe ser un número entre 1 y 1000000000.

Formato de tarjeta

Esta función está destinada exclusivamente a usuarios expertos. En cuanto se encienda el **Card format (Formato de tarjeta**:

- Si utiliza una credencial de 37 bits, se eliminan los últimos 5 bits.
- Si utiliza una credencial de 64 bits (código QR), se elimina la primera secuencia de 24 bits.

Puede utilizar tanto los datos de ejemplo como el lector de tarjetas para ver las credenciales.

1. Vaya a **Advanced (Avanzado)** > **Card format (Formato de tarjeta)**.
2. Lee la advertencia y haz clic en **I understand (Lo entiendo)** para habilitar el **Card format (Formato de tarjeta)**.
3. En el menú desplegable **Reader data visualization (Visualización de datos del lector)**, elija su lector.
4. Haga clic en **Get reader data (Obtener datos del lector)** o en **Use sample data (Utilizar datos de ejemplo)** para generar una salida de tarjeta. Se aplicará a todos los titulares de tarjetas registrados en el dispositivo.
5. Active la opción **Trim reader data (Recortar datos del lector)** para eliminar los bits finales de las credenciales de la tarjeta.
6. Haga clic en **Enable (Activar)**.

Mapas de campo

- **Name (Nombre)** (obligatorio): introduzca el nombre del mapa de campo sin espacios; por ejemplo, `OddParity`.
  Ejemplos de mapas de campo comunes:

  - `Parity`: los bits de paridad se utilizan para detectar errores. Los bits de paridad habitualmente se añaden al principio o al final de una cadena de código binario e indican si el número de bits es par o impar.
  - `EvenParity`: los bits de paridad par aseguran que la cadena contenga un número de bits par. Se cuentan los bits que tienen valor 1. Si el recuento ya es par, el valor del bit de paridad se establecerá en 0. Si el recuento es impar, el valor del bit de paridad par se establecerá en 1, convirtiendo el recuento total en un número par.
  - `OddParity`: los bits de paridad impar aseguran que la cadena contenga un número de bits impar. Se cuentan los bits que tienen valor 1. Si el recuento ya es impar, el valor del bit de paridad impar se establecerá en 0. Si el recuento es par, el valor del bit de paridad se establecerá en 1, convirtiendo el recuento total en un número impar.
  - `FacilityCode`: los códigos de instalación se utilizan en ocasiones para comprobar que el token coincide con el lote de credenciales de usuario final solicitado. En sistemas heredados de control de acceso, se utilizaba el código de instalación para una validación reducida, permitiendo el acceso a todos los empleados incluido en el lote de credenciales que se había codificado con un código de instalación coincidente. Este nombre de mapa de campo, sensible a mayúsculas y minúsculas, es requerido para que el producto valide un código de instalación.
  - `CardNr`: el número de tarjeta o ID de usuario es lo que habitualmente se valida en sistemas de control de acceso. Este nombre de mapa de campo, sensible a mayúsculas y minúsculas, es requerido para que el producto valide un número de tarjeta.
  - `CardNrHex`: los datos binarios del número de tarjeta se codifican en el producto como números hexadecimales en minúsculas. Se utiliza principalmente para solucionar problemas cuando no se obtiene el número de tarjeta esperado del lector.
- **Range (rango)** (requerido): introduzca el rango de bits del mapa de campo; por ejemplo, 1, 2-17, 18-33 y 34.
- **Encoding (Codificación)** (requerido): seleccione el tipo de codificación de cada mapa de campo.
  - **BinLE2Int**: los datos binarios se codifican como números enteros en orden de bits little-endian. Integer (entero) significa que debe ser un número entero (sin decimales). Orden de bits little-endian significa que el primer bit es el más pequeño (menos significativo).
  - **BinBE2Int**: los datos binarios se codifican como números enteros en orden de bits big-endian. Integer (entero) significa que debe ser un número entero (sin decimales). Orden de bits big-endian significa que el primer bit es el más grande (más significativo).
  - **BinLE2Hex**: los datos binarios se codifican como números hexadecimales en orden de bits little-endian. El sistema hexadecimal, también conocido como sistema numérico de base 16, consta de 16 símbolos únicos: los números del 0 al 9 y las letras de la a a la f. El orden de bits "little-endian" significa que el primer bit es el más pequeño (el menos significativo).
  - **BinBE2Hex**: los datos binarios se codifican como números hexadecimales en orden de bits big-endian. El sistema hexadecimal, también conocido como sistema numérico de base 16, consta de 16 símbolos únicos: los números del 0 al 9 y las letras de la a a la f. El orden de bits "big endian" significa que el primer bit es el más grande (el más significativo).
  - **BinLEIBO2Int**: los datos binarios se codifican del mismo modo que en BinLE2Int, pero los datos de tarjeta sin formato se leen en un orden de bytes invertido en una secuencia multibyte antes de obtener los mapas de campo para la codificación.
  - **BinBEIBO2Int**: los datos binarios se codifican del mismo modo que en BinBE2Int, pero los datos de tarjeta sin formato se leen en un orden de bytes invertido en una secuencia multibyte antes de obtener los mapas de campo para la codificación.

Para obtener información acerca de los mapa de campo que utiliza su formato de tarjeta, consulte las instrucciones del fabricante.

Configurar servicios

La función de configurar servicios, en la página de configuración, se utiliza para acceder a la configuración de los servicios externos que se pueden utilizar con el controlador de puerta.

SmartIntego

SmartIntego es una solución inalámbrica que aumenta el número de puertas que puede gestionar un controlador de puerta.

Requisitos previos de SmartIntego

Hay que reunir los requisitos previos siguientes antes de continuar con la configuración de SmartIntego:

- Hay que crear un archivo csv. El archivo csv contiene información sobre el GatewayNode y las puertas que se utilizan en la solución SmartIntego. El archivo se crea en un software autónomo proporcionado por un socio de SimonsVoss.
- Se ha completado la configuración de hardware de SmartIntego; consulte *Cómo crear una nueva configuración de hardware para cierres inalámbricos, on page 15*.

Nota

- La configuración de SmartIntego debe ser la versión 2.1.6452.23485, compilación 2.1.6452.23485 (31/8/2017 1:02:50 h) o posterior.
- El estándar de cifrado avanzado (AES) no es compatible con SmartIntego y, por lo tanto, debe estar desactivado en la configuración de SmartIntego.

Cómo configurar SmartIntego

Nota

- Asegúrese de que se han reunido los requisitos previos enumerados.
- Para una mayor visibilidad del estado de la batería, vaya a **Setup (Configuración)** > **Configure event and alarms logs (Configurar registros de eventos y alarmas)** y añada **Door — Battery alarm (Puerta — Alarma de batería)** o **IdPoint — Battery alarm (IdPoint — Alarma de batería)** como alarma.
- Los ajustes de monitor de puerta provienen del archivo CSV importado. No debería tener que cambiar este ajuste en una instalación normal.

1. Haga clic en **Browse... (Examinar...)**, seleccione el archivo csv y haga clic en **Upload file (Cargar archivo)**.
2. Seleccione un GatewayNode y haga clic en **Next (Siguiente)**.
3. Se muestra una vista previa de la nueva configuración. Desactive los monitores de puerta si fuese necesario.
4. Haga clic en **Configure (Configuración)**.
5. Se muestra una vista completa de las puertas incluidas en la configuración. Haga clic en **Settings (Configuración)** para configurar cada puerta individualmente.

Cómo configurar de nuevo SmartIntego

1. Haga clic en **Setup (Configuración)** en el menú superior.
2. Haga clic en **Configure Services (Configurar servicios)** > **Settings (Ajustes)**.
3. Haga clic en **Re-configure (Configurar de nuevo)**.
4. Haga clic en **Browse... (Examinar...)**, seleccione el archivo csv y haga clic en **Upload file (Cargar archivo)**.
5. Seleccione un GatewayNode y haga clic en **Next (Siguiente)**.
6. Se muestra una vista previa de la nueva configuración. Desactive los monitores de puerta si fuese necesario.

Nota

Los ajustes de monitor de puerta provienen del archivo CSV importado. No debería tener que cambiar este ajuste en una instalación normal.

7. Haga clic en **Configure (Configuración)**.
8. Se muestra una vista completa de las puertas incluidas en la configuración. Haga clic en **Settings (Configuración)** para configurar cada puerta individualmente.

Perfil LED OSDP

Puede personalizar los perfiles de los LED de su lector OSDP para definir las luces y los sonidos que se utilizan en función de los distintos eventos. Para consultar la lista completa de perfiles, véase *LED profiles (Perfiles LED)*.

Establecer niveles de luz y audio

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Despliegue el menú **Light and audio levels (Niveles de luz y audio)**.
3. Utilice el control deslizante para ajustar la intensidad de la tira de LED, la retroiluminación LED y el sonido.
4. Haga clic en **Save (Guardar)**.

Nota

Al cambiar los niveles de luz y audio, los ajustes se actualizan en todos los lectores conectados al controlador.

Comprobar los ajustes de los LED del OSDP:

Puede utilizar el menú **OSDP LED test (Prueba LED de OSDP)** para consultar los ajustes de audio e iluminación de cualquiera de sus perfiles de lector.

Para comprobar los ajustes de sus perfiles LED de OSDP:

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Despliegue el menú **OSDP LED test (Prueba LED de OSDP)**.
3. Elija un indicador LED.
4. Elija el lector que desea probar.
5. Haga clic en **Iniciar**.
6. Haga clic **Edit feedback (Editar respuesta)** para cambiar los ajustes de luz y audio de su perfil.
   - Elija un nuevo color en el menú desplegable **Color**.
   - Elija una frecuencia de audio en el menú desplegable **Audio**, si procede.
   - También puede restablecer los ajustes del perfil haciendo clic en **Reset to default values (Restablecer valores predeterminados)**.
   - Haga clic en **Save (Guardar)**.

Cambiar los ajustes del perfil LED de OSDP:

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Acceda al **OSDP LED profile (Perfil LED de OSDP)**.
3. Haga clic en junto al perfil que desea editar.
4. Edite los ajustes correspondientes:
   - Elija el comportamiento que seguirán sus LED en el menú desplegable **Behaviour (Comportamiento)**.
   - Elija el color de sus LED en el menú desplegable **Color**.
   - Establezca la **Duration on (Duración de encendido)** y la **Duration off (Duración de apagado)** de sus LED.
   - Establezca la **Recurrence (Periodicidad)** de la respuesta del LED.

- En el menú desplegable **Audio**, elija la **Beep duration, on (Duración del pitido, encendido)** y la **Beep duration, off (Duración del pitido, apagado)** y determine la**Recurrence (Periodicidad)** de la respuesta del avisador acústico. Asegúrese de que la **Beep duration, on (Duración del pitido, encendido)** y la **Beep duration, off (Duración del pitido, apagado)** sean iguales.

5. Haga clic en **Save (Guardar)**.

Importar ajustes existentes desde otro controlador

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Haga clic en **Import (Importar)**.
3. Seleccione el archivo que desea subir.
4. Haga clic en **Import (Importar)**.

Exportar los ajustes actuales

1. Vaya a **Peripherals (Periféricos)** > **Readers (Lectores)** > **OSDP LED profile (Perfil LED OSDP)**.
2. Haga clic en **Export (Exportar)**.
3. Elija dónde desea guardar el archivo JSON y haga clic en **Save (Guardar)**.

Instrucciones de mantenimiento

Para mantener el sistema de control de acceso funcionando correctamente, Axis recomienda efectuarle un mantenimiento periódico, incluidos los controladores de puerta y los dispositivos conectados.

Efectúe tareas de mantenimiento al menos una vez al año. El procedimiento de mantenimiento sugerido incluye, aunque sin limitarse a ellos, los siguientes pasos:

- Compruebe que todas las conexiones entre el controlador de puerta y los dispositivos externos sean seguras.
- Verifique todas las conexiones de hardware. Consulte *Verificación de controles de puertas, on page 17*.
- Compruebe que el sistema funcione correctamente, incluidos los dispositivos externos conectados.

– Pase una tarjeta y pruebe los lectores, las puertas y las cerraduras.

– Si el sistema incluye dispositivos REX, sensores u otros dispositivos, pruébelos también.

– Si están activadas, pruebe también las alarmas antimanipulación.

Si los resultados de cualquiera de los pasos anteriores indican que hay fallos o comportamientos inesperados:

– Pruebe las señales de los cables usando los equipos adecuados y compruebe si los cables están dañados en algún sentido.

– Sustituya todos los cables defectuosos.

– Una vez que se hayan sustituido los cables, compruebe de nuevo las conexiones de hardware. Consulte *Verificación de controles de puertas, on page 17*.

- Si el controlador de puerta no actúa del modo previsto, consulte *Localización de problemas, on page 38* y *Maintenance (Mantenimiento):, on page 35* para obtener más información.

Configuración de eventos

Los eventos que se producen en el sistema, por ejemplo cuando un usuario pasa una tarjeta o se activa un dispositivo REX, se registran en el registro de eventos.

- Ver el registro de eventos. Consulte *page 24*.
- Exportar el registro de eventos. Consulte .
- Configurar el registro de eventos. Consulte *Configurar el registro de eventos, on page 24*.

Ver el registro de eventos

Para ver los eventos registrados, vaya a **Event Log (Registro de eventos)**.

Para expandir un elemento en el registro de eventos y ver los detalles del evento, haga clic en .

Aplicar filtros al registro de eventos facilita encontrar eventos específicos. Para filtrar la lista, seleccione uno o varios filtros del registro de eventos y haga clic en **Apply filters (Aplicar filtros)**. Para obtener más información, consulte *Filtros de registro de eventos, on page 24*.

Como administrador, puede tener más interés en determinados eventos que en otros. De este modo, puede elegir los eventos que se deben registrar. Para obtener más información, consulte *Opciones del registro de eventos, on page 24*.

Filtros de registro de eventos

Puede restringir el alcance del registro de eventos seleccionando uno o varios de los siguientes filtros:

- Usuario: filtrar por eventos relacionados con un usuario seleccionado.
- Puerta y planta: filtrar por eventos relacionados con una puerta o planta específicas.
- Asunto: filtrar por tipo de evento.
- Fecha y hora: filtrar el registro de eventos por una fecha e intervalo horario.

Configurar el registro de eventos

La página Configurar el registro de eventos permite definir qué eventos se registrarán.

Opciones del registro de eventos

Para definir los eventos que se incluirán en el registro de eventos, vaya a **Setup > Configure Event Logs (Configuración > Configurar registros de eventos)**.

Las siguientes opciones para el registro de eventos están disponibles:

- **No logging (Ningún registro)**: deshabilita el registro de eventos. El evento no se registrará ni se incluirá en el registro de eventos.
- **Log for all sources (Registro para todas las fuentes)**: habilita el registro de eventos. El evento se registrará y se incluirá en el registro de eventos.

Cómo configurar reglas de acción

Las páginas de eventos permiten configurar el producto de Axis para realizar acciones al producirse distintos eventos. El conjunto de condiciones que define cómo y cuándo se activa la acción se denomina regla de acción. Si se definen varias condiciones, todas ellas deberán cumplirse para que se active la acción.

Para obtener más información acerca de los desencadenadores y acciones disponibles, consulte la ayuda integrada del producto.

En este ejemplo se describe cómo configurar una regla de acción para activar un puerto de salida cuando la puerta ha sido forzada.

1. Vaya a **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Configuración > Configuración de controlador adicional > Opciones del sistema > Puertos y dispositivos > Puertos de E/S)**.
2. Seleccione **Salida** en el elemento deseado de la lista desplegable **Tipo de puerto de E/S** e introduzca un **Nombre**.
3. Seleccione el **Estado Normal** del puerto de salida E/S y haga clic en **Guardar**.
4. Vaya a **Events > Action Rules (Eventos > Reglas de acción)** y haga clic en **Add (Añadir)**.
5. Seleccione **Puerta** en la lista desplegable **Activador**.
6. Seleccione **Alarma de puerta** en la lista desplegable.
7. Seleccione la puerta deseada en la lista desplegable.
8. Seleccione **Puerta forzada** en la lista desplegable.
9. Si lo desea, seleccione una **Programación** y **Condiciones adicionales**. Más detalles a continuación.
10. En **Acciones**, seleccione **Puerto de salida** en la lista desplegable **Tipo**.
11. Seleccione el puerto de salida deseado en la lista desplegable **Puerto**.
12. Establezca el estado en **Activo**.
13. Seleccione **Duración** e **Ir después al estado opuesto**. A continuación, introduzca la duración deseada de la acción.
14. Haga clic en **OK**.

Para utilizar más de un activador para la regla de acción, seleccione **Condiciones adicionales** y haga clic en **Añadir** para añadir desencadenadores adicionales. Al utilizar condiciones adicionales, todas las condiciones deben cumplirse para que se active la acción.

Para evitar que una acción se active repetidamente, se puede establecer un tiempo mínimo de espera en **Esperar al menos**. Introduzca el tiempo en horas, minutos y segundos, durante el cual debe ignorarse el activador antes de que la regla de acción se pueda activar de nuevo.

Para obtener más información, consulte la ayuda integrada del producto.

Cómo añadir destinatarios

El producto puede enviar mensajes para notificar a los destinatarios acerca de eventos y alarmas. Pero antes de que el producto puede enviar mensajes de notificación, se deben definir uno o varios destinatarios. Para obtener más información sobre las opciones disponibles, consulte .

Para añadir un destinatario:

1. Vaya a **Setup > Additional Controller Configuration > Events > Recipients (Configuración > Configuración de controlador adicional > Eventos > Destinatarios)** y haga clic en **Añadir**.
2. Introduzca un nombre descriptivo.
3. Seleccione un **tipo** de destinatario.
4. Introduzca la información necesaria para el tipo de destinatario.
5. Haga clic en **Prueba** para probar la conexión con el destinatario.
6. Haga clic en **OK**.

Cómo configurar destinatarios de correo electrónico

Los destinatarios de correo electrónico se pueden configurar seleccionando uno de los proveedores de correo electrónico enumerados o especificando el servidor SMTP, el puerto y la autentificación utilizada, por ejemplo, por un servidor de correo electrónico corporativo.

Nota

Algunos proveedores de correo electrónico cuentan con filtros de seguridad que evitan que los usuarios reciban o archivos adjuntos de gran tamaño, que reciban correos programados, etc. Compruebe la política de seguridad del proveedor de correo electrónico para evitar problemas de entrega y bloqueos en las cuentas de correo electrónico.

Para configurar un destinatario de correo electrónico mediante uno de los proveedores enumerados:

1. Vaya a **Events > Recipients (Eventos > Destinatarios)** y haga clic en **Add (Añadir)**.
2. Introduzca un **Name (Nombre)** y seleccione **Email (Correo electrónico)** en la lista **Type (Tipo)**.
3. Introduzca las direcciones de correo electrónico a las que se enviarán mensajes de correo electrónico en el campo **To (Para)**. Utilice comas para separar múltiples direcciones.
4. Seleccione un proveedor de correo electrónico en la lista **Provider (Proveedor)**.
5. Introduzca la ID de usuario y la contraseña de la cuenta de correo electrónico.
6. Haga clic en **Test (Probar)** para enviar un correo electrónico de prueba.

Para configurar un destinatario de correo electrónico mediante, por ejemplo, un servidor de correo electrónico corporativo, siga las instrucciones anteriores, pero seleccione **User defined (Definido por el usuario)** como **Provider (Proveedor)**. Introduzca la dirección de correo electrónico que aparecerá como remitente en el campo **From (De)**. Seleccione **Advanced settings (Configuración avanzada)** y especifique el servidor SMTP, el puerto y el método de autentificación. Opcionalmente, seleccione **Use encryption (Utilizar cifrado)** para enviar mensajes de correo electrónico a través de una conexión cifrada. El certificado de servidor puede ser validado mediante los certificados disponibles en el producto de Axis. Para obtener información sobre cómo cargar certificados, consulte *Certificados, on page 29*.

Cómo crear programaciones

Las programaciones se pueden utilizar como activadores de reglas de acción o como condiciones adicionales. Utilice una de las programaciones predefinidas o cree una nueva programación según se describe a continuación.

Para crear una nueva programación:

1. Vaya a **Setup > Additional Controller Configuration > Events > Schedules (Configuración > Configuración de controlador adicional > Eventos > Programaciones)** y haga clic en **Añadir**.
2. Introduzca un nombre descriptivo y la información necesaria para una programación diaria, semanal, mensual o anual.
3. Haga clic en **OK**.

Para utilizar la programación en una regla de acción, seleccione la programación en la lista desplegable **Programación** en la página de configuración de la regla de acción.

Cómo configurar repeticiones

Las repeticiones se utilizan para activar la reglas de acción varias veces, por ejemplo, cada 5 minutos o cada hora.

Para configurar una repetición:

1. Vaya a **Setup > Additonal Controller Configuration > Events > Recurrences (Configuración > Configuración de controlador adicional > Eventos > Repeticiones)** y haga clic en **Añadir**.
2. Especifique un nombre descriptivo y un patrón de repetición.
3. Haga clic en **OK**.

Para usar la repetición en una regla de acción, seleccione en primer lugar **Tiempo** en la lista desplegable **Activador** en la página Configuración de regla de acción y, a continuación, seleccione la repetición en la segunda lista desplegable.

Para modificar o eliminar las repeticiones, seleccione la repetición en la **Lista de repeticiones** y haga clic en **Modificar** o en **Eliminar**.

Información del lector

Los lectores utilizan luces LED e indicadores acústicos para enviar información al usuario (la persona que accede o intenta acceder a la puerta). El controlador de puerta puede activar una serie de mensajes informativos, algunos de los cuales se han preconfigurado en el controlador de puerta y son compatibles con la mayoría de lectores.

Los lectores presentan diferentes respuestas LED, pero por lo general utilizan distintas secuencias de luces fijas y parpadeantes de color rojo, verde y ámbar.

Los lectores también pueden utilizar indicadores acústicos de un solo tono para enviar mensajes mediante distintas secuencias de señales acústicas cortas y largas.

La tabla siguiente muestra los eventos preconfigurados en el controlador de puerta para activar la información del lector y sus señales de información más habituales. Las señales informativas de los lectores de Axis se presentan en la guía de instalación proporcionada con el lector de Axis.

Evento	Wiegand LED doble	Wiegand LED simple	OSDP	Patrón de indicador acústico	Estado
En reposo[1]	Apagado	Rojo	Rojo	Silencioso	Normal
Se requiere PIN	Rojo/verde intermitente	Rojo/verde intermitente	Rojo/verde intermitente	Dos pitidos cortos	Se requiere PIN
Acceso permitido	Verde	Verde	Verde	Bip	Acceso permitido
Acceso denegado	Rojo	Rojo	Rojo	Bip	Acceso denegado

Los mensajes de información distintos de los anteriores se deben configurar mediante un cliente, como un sistema de gestión de acceso, a través de la interfaz de programación de aplicaciones VAPIX®, que es compatible con esta función y utiliza lectores capaces de proporcionar las señales requeridas. Para obtener más información, consulte la información del usuario proporcionada por el desarrollador del sistema de gestión de acceso y por el fabricante del lector.

1. *Se pasa a estado inactivo cuando la puerta está cerrada y la cerradura esté bloqueada.*

Opciones del sistema

Seguridad

Usuarios

El control de acceso de usuario está activado de forma predeterminada y se pueden configurar en **Setup > Additional Controller Configuration > System Options > Security > Users (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Usuarios)**. Un administrador puede configurar otros usuarios asignándoles nombres de usuario y contraseñas.

La lista de usuarios muestra los usuarios autorizados y grupos de usuarios (niveles de acceso):

- **Los administradores** tienen acceso sin restricciones a todos los ajustes. El administrador puede añadir, modificar y eliminar otros usuarios.

Nota

Tenga en cuenta que, cuando la opción **Cifrado y sin cifrar** está activada, el servidor web cifrará la contraseña. Esta es la opción predeterminada para una unidad nueva o para una unidad restablecida a los ajustes predeterminados de fábrica.

En **Configuración de contraseña HTTP/RTSP**, seleccione el tipo de contraseña permitida. Puede que necesite permitir contraseñas no cifradas si hay clientes de visualización que no admiten cifrado o si ha actualizado el firmware y los clientes actuales admiten cifrado, pero se debe volver a iniciar sesión para configurarlos a fin de utilizar esta funcionalidad.

ONVIF

ONVIF es un foro abierto del sector que proporciona y promueve interfaces estandarizadas para una eficiente interoperabilidad de los productos de seguridad físicos basados en IP.

Al crear un usuario, se permite automáticamente la comunicación ONVIF. Utilice el nombre de usuario y la contraseña en todas las comunicaciones ONVIF con el producto. Consulte *www.onvif.org* para obtener más información.

Filtro de direcciones IP

El filtrado de direcciones IP se habilita en la página **Setup > Additional Controller Configuration > System Options > Security > IP Address Filter (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Filtro de direcciones IP)**. Una vez activado, el acceso al producto de Axis está permitido o denegado a las direcciones IP enumeradas. Seleccione en la lista **Permitir** o **Denegar** y haga clic en **Aplicar** para habilitar el filtrado de direcciones IP.

El administrador puede añadir a la lista hasta 256 entradas de direcciones IP (una única entrada puede incluir varias direcciones IP).

HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, o HTTP por SSL) es un protocolo web que proporciona navegación cifrada. Los usuarios y clientes también pueden utilizar HTTPS para comprobar que se tiene acceso al dispositivo correcto. El nivel de seguridad proporcionado por HTTPS se considera adecuado para la mayoría de intercambios comerciales.

El producto de Axis puede configurarse para solicitar HTTPS cuando los administradores inician sesión.

Para poder usar HTTPS, debe haber instalado un certificado HTTPS. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)** para instalar y administrar certificados. Consulte *Certificados, on page 29*.

Para habilitar HTTPS en el producto de Axis:

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > HTTPS)**
2. Seleccione un certificado HTTPS en la lista de certificados instalados.
3. Opcionalmente, haga clic en **Ciphers (Cifrados)** y seleccione los algoritmos de cifrado que se utilizarán para SSL.
4. Establezca la **HTTPS Connection Policy (Política de conexión HTTPS)** para los distintos grupos de usuarios.
5. Haga clic en **Save (Guardar)** para activar la configuración.

Para acceder al producto de Axis a través del protocolo deseado, introduzca en el campo de dirección del navegador `https://` para el protocolo HTTPS y `http://` para el protocolo HTTP.

Se puede cambiar el puerto HTTPS en la página **System Options > Network > TCP/IP > Advanced (Opciones del sistema > Red > TCP/IP > Avanzadas)** página.

IEEE 802.1X

IEEE 802.1X es un estándar para el control de admisión de red basada en puertos que proporciona una autenticación segura de los dispositivos de red conectados e inalámbricos. IEEE 802.1x se basa en el EAP (protocolo de autentificación extensible).

Para acceder a una red protegida por IEEE 802.1X, los dispositivos deben autenticarse. Un servidor de autenticación lleva a cabo esta autenticación, normalmente un **servidor RADIUS**; por ejemplo, FreeRADIUS y Microsoft Internet Authentication Server.

En la implementación de Axis, el producto de Axis y el servidor de identificación se identifican ellos mismos con certificados digitales utilizando EAP-TLS (protocolo de autenticación extensible - seguridad de la capa de transporte). Los certificados son proporcionados por una **Autoridad de Certificación** (AC). Necesitará:

- Un certificado de la AC para autenticar el servidor de autenticación.
- Un certificado de cliente con firma AC para autenticar el producto de Axis.

Para crear e instalar certificados, vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)** para instalar y administrar certificados. Consulte *Certificados, on page 29*.

Para permitir el acceso del producto a una red protegida por IEEE 802.1X:

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > IEEE 802.1X (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > IEEE 802.1X)**.
2. Seleccione un **CA Certificate (Certificado de AC)** y un **Client Certificate (Certificado de cliente)** de las listas de certificados instalados.
3. En **Settings (Ajustes)**, seleccione la versión EAPOL y proporcione la identidad EAP asociada al certificado de cliente.
4. Marque la casilla para activar IEEE 802.1X y haga clic en **Save (Guardar)**.

Nota

Para que la autentificación funcione correctamente, la configuración de fecha y hora del producto de Axis se debe sincronizar con un servidor NTP. Consulte .

Certificados

Los certificados se utilizan para autenticar los dispositivos de una red. Las aplicaciones más habituales incluyen la navegación web cifrada (HTTPS), la protección de la red mediante IEEE 802.1X y los mensajes de notificación, por ejemplo a través de correo electrónico. Se pueden utilizar dos tipos de certificados con los productos de Axis:

Server/Client certificates (Certificados de servidor-cliente) – Autenticar el producto Axis. Un certificado **Server/Client (Servidor-Cliente)** puede ser autofirmado o emitido por una autoridad de certificación (AC). Un certificado firmado por el propio producto ofrece protección limitada y se puede utilizar antes de que se obtenga un certificado emitido por una autoridad de certificación.

Certificados de autoridad de certificación – Autenticar certificados entre iguales, por ejemplo, el certificado de un servidor de autenticación en caso de que el producto de Axis se conecte a una red protegida IEEE 802.1X. El producto de Axis se proporciona con varios certificados AC preinstalados.

Nota

- Si el producto se restablece a la configuración predeterminada de fábrica, se eliminarán todos los certificados, excepto los certificados AC preinstalados.
- Si el producto se restablece a la configuración predeterminada de fábrica, se reinstalarán todos los certificados, excepto los certificados AC preinstalados.

Cómo crear un certificado autofirmado

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)**.
2. Haga clic en **Create self-signed certificate (Crear certificado autofirmado)** y proporcione la información solicitada.

Cómo crear e instalar un certificado firmado por una autoridad de certificación

1. Cree un certificado autofirmado; consulte *Cómo crear un certificado autofirmado, on page 30*.
2. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)**.
3. Haga clic en **Create certificate signing request (Crear solicitud de firma de certificado)** y proporcione la información solicitada.
4. Copie la solicitud con formato PEM y envíela a la autoridad de certificación de su elección.
5. Cuando se devuelva el certificado firmado, haga clic en **Install certificate (Instalar certificado)** y cargue el certificado).

Cómo instalar certificados adicionales de una autoridad de certificación

1. Vaya a **Setup > Additional Controller Configuration > System Options > Security > Certificates (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > Certificados)**.
2. Haga clic en **Install certificate (Instalar certificado)** y cargue el certificado.

Red

Ajustes básicos de TCP/IP

El producto de Axis admite IP versión 4 (IPv4) e IP versión 6 (IPv6).

El producto de Axis puede obtener una dirección IP de los siguientes modos:

- **Dirección IP dinámica**: **Obtain IP address via DHCP (Obtener dirección IP a través de DHCP)** está activado de forma predeterminada. Esto significa que se configura el producto Axis para que obtenga automáticamente la dirección IP a través de Dynamic Host Configuration Protocol (DHCP).
  DHCP permite a los administradores de red administrar y automatizar la asignación de direcciones IP de forma centralizada.
- **Dirección IP estática** : para utilizar una dirección IP estática, seleccione **Use the following IP address (Usar la siguiente dirección IP)** y especifique la dirección IP, la máscara de subred y el router predeterminado. A continuación, haga clic en **Save (Guardar)**.

DHCP solo debe habilitarse si se utiliza la notificación de dirección IP dinámica o si DHCP puede actualizar un servidor DNS que permite acceder al producto de Axis por su nombre (nombre de host).

Si DHCP está habilitado y no se puede acceder al producto, ejecute AXIS IP Utility para buscar en la red los productos Axis conectados, o restablezca el producto a la configuración predeterminada de fábrica y, a continuación, vuelva a realizar la instalación. Para obtener información sobre cómo restablecer los valores predeterminados de fábrica, consulte *page 38*.

AXIS Video Hosting System (AVHS)

AVHS, utilizado en combinación con un servicio AVHS, ofrece acceso seguro y sencillo a Internet para poder acceder a la gestión del controlador y los registros desde cualquier ubicación. Para obtener más información y asistencia para localizar un proveedor de servicios AVHS, acceda a www.axis.com/hosting.

Los ajustes de AVHS se configuran en **Setup > Additional Controller Configuration > System Options > Network > TCP IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP IP > Básica)**. La posibilidad de conectarse a un servicio AVHS está activada de forma predeterminada. Para deshabilitarla, desmarque la casilla **Habilitar AVHS**.

Habilitar un solo clic – Mantenga pulsado el botón de control del producto (consulte *Guía de productos, on page 6*) durante aproximadamente 3 segundos para conectar a un servicio AVHS a través de Internet. Una vez registrado, debe habilitarse **Siempre** y el producto de Axis permanecerá conectado al servicio AVHS. Si no se registra el producto en un plazo de 24 horas desde el momento en que se pulsó el botón, el producto se desconectará del servicio AVHS.

Siempre – El producto de Axis intentará conectarse continuamente al servicio AVHS a través de Internet. Una vez registrado, el producto permanecerá conectado al servicio. Esta opción puede utilizarse cuando el producto ya está instalado y no es posible o no es conveniente utilizar la instalación en un solo clic.

Nota

El soporte de AVHS depende de la disponibilidad de suscripciones de proveedores de servicios.

Servicio AXIS Internet Dynamic DNS

El servicio AXIS Internet Dynamic DNS asigna un nombre de host para facilitar el acceso al producto. Para obtener más información, consulte *www.axiscam.net*

Para registrar el producto de Axis en el servicio AXIS Internet Dynamic DNS, vaya a **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Básica)**. En **Servicios**, haga clic en el botón **Configuración** de AXIS Internet Dynamic DNS Service (requiere acceso a Internet). El nombre de dominio registrado actualmente en el servicio AXIS Internet Dynamic DNS para el producto se puede eliminar en cualquier momento.

Nota

AXIS Internet Dynamic DNS Service requiere IPv4.

Advanced TCP/IP Settings

Configuración de DNS

DNS (Domain Name Service) proporciona la traducción de nombres de host a direcciones IP. Los ajustes DNS se configuran desde **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada)**.

Seleccione **Obtain DNS server address via DHCP (Obtener dirección de servidor DNS a través de DHCP)** para utilizar la configuración de DNS proporcionada por el servidor DHCP.

Para realizar la configuración manual, seleccione **Use the following DNS server address (Usar la siguiente dirección del servidor DNS)** y especifique los elementos siguientes:

Nombre de dominio – Introduzca los dominios donde se buscará el nombre de host utilizado por el producto Axis. Se pueden introducir múltiples dominios separados por punto y coma. El nombre de host siempre es la primera parte de un nombre de dominio completamente cualificado; por ejemplo, `myserver` es el nombre de host en el nombre de dominio completamente cualificado `myserver.mycompany.com`, donde `mycompany.com` es el nombre de dominio.

Servidor DNS principal y secundario – Introduzca las direcciones IP de los servidores DNS principal y secundario. El servidor DNS secundario es opcional y se utilizará cuando el principal no esté disponible.

Configuración de NTP

NTP (Network Time Protocol) se utiliza para sincronizar la hora de reloj de los dispositivos de una red. Los ajustes NTP se configuran desde **Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada (Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced)**.

Seleccione **Obtain NTP server address via DHCP (Obtener dirección de servidor NTP a través de DHCP)** para utilizar la configuración de NTP proporcionada por el servidor DHCP.

Para realizar la configuración manual, seleccione **Use the following NTP server address (Usar la siguiente dirección de servidor NTP)** e introduzca el nombre de host o la dirección IP del servidor NTP.

Configuración de nombre de host

El producto de Axis es accesible a través de un nombre de host en lugar de una dirección IP. El nombre de host suele ser el mismo que el nombre DNS asignado. Esta función se configura en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**.

Seleccione **Obtain host name via IPv4 DHCP (Obtener nombre de host a través de DHCP IPv4)** para utilizar el nombre de host proporcionado por el servidor DHCP que se ejecuta en IPv4.

Seleccione **Use the host name (Utilizar el nombre de host)** para establecer manualmente el nombre de host.

Seleccione **Enable dynamic DNS updates (Activar actualizaciones dinámicas de DNS)** para actualizar dinámicamente los servidores DNS locales siempre que cambie la dirección IP del producto de Axis. Consulte la ayuda en línea para obtener más información.

Dirección IPv4 de enlace-local

Link-Local Address (Dirección de enlace local) se activa de forma predeterminada y asigna al producto de Axis una dirección IP adicional que se puede utilizar para acceder al producto desde otros hosts en el mismo segmento de la red local. El producto puede tener una IP de enlace local y al mismo tiempo una dirección IP estática o proporcionada por DHCP.

Esta función se puede deshabilitar en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración del controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**.

HTTP

El puerto HTTP utilizado por el producto de Axis se puede cambiar en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**. Además del puerto predeterminado, que es 80, se puede utilizar cualquier puerto entre 1024 y 65535.

HTTPS

El puerto HTTPS utilizado por el producto de Axis se puede cambiar en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**. Además del puerto predeterminado, que es 443, se puede utilizar cualquier puerto entre 1024 y 65535.

Para activar HTTPS, vaya a **Setup > Additional Controller Configuration > System Options > Security > HTTPS (Configuración > Configuración de controlador adicional > Opciones del sistema > Seguridad > HTTPS)**. Para obtener más información, consulte *HTTPS, on page 28*.

NAT transversal (asignación de puertos) para IPv4

Un router de red permite a los dispositivos en una red privada (LAN) compartir una única conexión a Internet. Esto se realiza redirigiendo el tráfico de red desde la red privada hacia el "exterior", es decir, hacia internet. La seguridad de la red privada (LAN) es mayor, ya que la mayoría de los routers están preconfigurados para detener los intentos de acceso a la red privada (LAN) desde la red pública (internet).

Utilice **NAT transversal** cuando el producto Axis se encuentra en una intranet (LAN) y se desea que esté disponible desde el otro lado (WAN) de un router NAT. Con la NAT transversal configurada correctamente, se envía al producto todo el tráfico HTTP a un puerto externo HTTP en el router NAT.

NAT transversal se configura desde **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada)**.

Nota

- La NAT transversal debe ser compatible con el router para poder funcionar. El router debe ser compatible también con UPnP®.
- En este contexto, un router hace referencia a cualquier dispositivo de enrutamiento de red, como un router NAT, un router de red, una puerta de enlace de Internet, un router de banda ancha, un dispositivo de uso compartido de banda ancha o un software, como un cortafuegos.

Activar/desactivar – Si se activa, el producto de AXIS tratará de configurar la asignación de puertos de un router NAT de la red mediante UPnP. Tenga en cuenta que UPnP debe estar habilitado en el producto (consulte **Setup > Additional Controller Configuration > System Options > Network > UPnP (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > UPnP)**).

Utilizar router NAT seleccionado manualmente – Seleccione esta opción para seleccionar manualmente un router NAT y escriba en el campo la dirección IP para el router. Si no se especifica ningún router, el producto busca automáticamente routers NAT en su red. Si se encuentra más de un router, se selecciona el router predeterminado.

Puerto HTTP alternativo – Seleccione esta opción para definir manualmente un puerto HTTP externo. Introduzca un puerto dentro del rango 1024-65535. Si el campo del puerto está vacío o contiene la configuración predeterminada, que es 0, se seleccionará automáticamente un número de puerto al habilitar NAT transversal.

Nota

- Un puerto HTTP alternativo puede utilizarse o estar activo incluso si la función de NAT transversal está desactivada. Esto resulta útil si el router NAT no admite UPnP y se necesita configurar manualmente la redirección de puertos en el router NAT.
- Si se intenta introducir manualmente un puerto que ya está en uso, automáticamente se selecciona otro puerto disponible.
- En este campo se indica si el puerto está seleccionado automáticamente. Para cambiarlo, introduzca un nuevo número de puerto y haga clic en **Guardar**.

FTP

El servidor FTP que se ejecuta en el producto Axis habilita la carga de nuevo firmware, aplicaciones de usuario, etc. El servidor FTP se puede desactivar desde **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de dispositivo adicional > Opciones de sistema > red > TCP/IP > Avanzada)**.

RTSP

El servidor RTSP que se ejecuta en el producto de Axis permite a un cliente conectado iniciar una transmisión de evento. Se puede cambiar el número de puerto RTSP en **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Advanced (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Avanzada)**. El puerto predeterminado es 554.

Nota

La retransmisión de eventos no estará disponible si se desactiva el servidor RTSP.

SOCKS

SOCKS es un protocolo de proxy de red. El producto de Axis puede configurarse para utilizar un servidor SOCKS a fin de llegar a redes situadas detrás de un cortafuegos o un servidor proxy. Esta funcionalidad resulta útil si el producto de Axis se encuentra en una red local detrás de un firewall y las notificaciones, cargas, alarmas, etc. deben enviarse a un destino situado fuera de la red local (por ejemplo, Internet).

SOCKS se configura en **Setup > Additional Controller Configuration > System Options > Network > SOCKS (Configuración > Configuración de controlador adicional > Opciones de sistema > Red > SOCKS)**. Consulte la ayuda en línea para obtener más información.

Calidad de Servicio (QoS)

QoS (calidad de servicio) garantiza un nivel determinado de un recurso especificado al tráfico seleccionado en una red. Una red con QoS establece las prioridades del tráfico de red y ofrece una mayor fiabilidad de la red mediante el control de la cantidad de ancho de banda que puede usar una aplicación.

La configuración de QoS se ajusta en **Setup > Additional Controller Configuration > System Options > Network > QoS (Configuración > Configuración de controlador adicional > Opciones de sistema > Red > QoS)**. Utilizando valores DSCP (Differentiated Services Codepoint), el producto de Axis puede marcar eventos/alarmas y gestión de tráfico.

SNMP

El protocolo de administración de red simple (SNMP) permite gestionar dispositivos de red de manera remota. Una comunidad SNMP es el grupo de dispositivos y estación de administración que ejecuta SNMP. Los nombres de comunidad se utilizan para identificar grupos.

Para habilitar y configurar SNMP en el producto de Axis, vaya a la página **Setup > Additional Controller Configuration > System Options > Network > SNMP (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > SNMP)**.

En función del nivel de seguridad requerido, seleccione la versión de SNMP que se utilizará.

El producto Axis utiliza traps para enviar mensajes al sistema de gestión ante eventos importantes y cambios de estado. Marque **Activar traps** e introduzca la dirección IP a la que se debe enviar el mensaje trap y la **Comunidad trap** que debe recibir el mensaje.

Nota

Si HTTPS está habilitado, SNMP v1 y SNMP v2c deben desactivarse.

El producto Axis utiliza **traps para SNMP v1/v2** a fin de enviar mensajes al sistema de gestión ante eventos importantes y cambios de estado. Marque **Activar traps** e introduzca la dirección IP a la que se debe enviar el mensaje trap y la **Comunidad trap** que debe recibir el mensaje.

Están disponibles las traps siguientes:

- Arranque en frío
- Arranque en caliente
- Vincular
- Error de autenticación

SNMP v3 proporciona cifrado y contraseñas seguras. Para usar traps con SNMP v3, se requiere una aplicación de administración de SNMP v3.

Para usar SNMP v3, HTTPS debe estar activado; consulte *HTTPS, on page 28*. Para habilitar SNMP v3, active la casilla de verificación y proporcione la contraseña del usuario inicial.

Nota

La contraseña inicial solo se puede establecer una vez. Si se pierde la contraseña, se deberá restablecer el producto Axis a su configuración predeterminada de fábrica; consulte *Restablezca la configuración predeterminada de fábrica, on page 38*.

UPnP

El producto de Axis incluye compatibilidad con UPnP®. UPnP está activado de forma predeterminada y el producto es detectado automáticamente por los sistemas operativos y clientes compatibles con este protocolo.

Se puede desactivar UPnP en **Setup > Additional Controller Configuration > System Options > Network > UPnP (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > UPnP)**.

Bonjour

El producto de Axis incluye compatibilidad con Bonjour. Bonjour está activado de forma predeterminada y el producto es detectado automáticamente por los sistemas operativos y clientes compatibles con este protocolo.

Se puede desactivar Bonjour en **Setup > Additional Controller Configuration > System Options > Network > Bonjour (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > Bonjour)**.

Puertos y dispositivos

Puertos de E/S

El conector auxiliar ofrece cuatro puertos de entrada y salida configurables para la conexión de dispositivos externos.

El conector externo ofrece dos puertos de entrada y salida configurables para la conexión de dispositivos externos.

Puede configurar los puertos de E/S en **Setup > Additional Controller Configuration > System Options > Ports & Devices > I/O Ports (Configuración > Configuración de controlador adicional > Opciones del sistema > Puertos y dispositivos > Puertos de E/S)**. Seleccione la dirección del puerto [**Input (Entrada)** o **Output (Salida)**]. Puede dar nombres descriptivos a los puertos y su **Normal state (Estado normal)** se puede configurar como **Open circuit (Circuito abierto)** o como **Grounded circuit (Circuito a tierra)**.

Estado de puerto

La lista que se encuentra en la página **System Options > Ports & Devices > Port Status (Opciones del sistema > Puertos y dispositivos > Estado de puerto)** muestra el estado de los puertos de entrada y salida del producto.

Maintenance (Mantenimiento):

El producto de Axis ofrece varias funciones de mantenimiento. Están disponibles en **Setup > Additional Controller Configuration > Setup > System Options > Maintenance (Configuración > Configuración del controlador adicional > Configuración > Opciones del sistema > Mantenimiento)**.

Haga clic en **Restart (Reiniciar)** para realizar un reinicio adecuado del producto Axis si este no se comporta como se espera. No afectará a la configuración actual.

Nota

Un reinicio borra todas las entradas en el informe del servidor.

Haga clic en **Restore (Restaurar)** para restablecer la mayoría de los ajustes a los valores predeterminados de fábrica. Los siguientes ajustes no se verán afectados:

- el protocolo de arranque (DHCP o estático)
- la dirección IP estática
- el router predeterminado
- la máscara de subred
- la hora del sistema
- los ajustes de IEEE 802.1X

Haga clic en **Default (Predeterminada)** para restablecer todos los valores, incluida la dirección IP, a los valores predeterminados de fábrica. Este botón debe utilizarse con precaución. El producto de Axis también se puede restablecer a los valores predeterminados de fábrica con el botón de control; consulte *Restablezca la configuración predeterminada de fábrica, on page 38*.

Para obtener información sobre la actualización del firmware, consulte *Cómo actualizar el firmware, on page 38*.

Asistencia técnica

Soporte de vista general

La página **Setup > Additional Controller Configuration > System Options > Support > Support Overview (Configuración > Configuración de controlador adicional > Opciones del sistema > Soporte > Soporte de vista general)** proporciona información para la localización de problemas e información de contacto en caso de necesitar asistencia técnica.

Consulte también *Localización de problemas, on page 38*.

Descripción del sistema

Para obtener una visión general de la configuración y el estado del producto de Axis, vaya a **Setup > Additional Controller Configuration > System Options > Support > System Overview (Configuración > Configuración de controlador adicional > Opciones del sistema > Soporte > Descripción general del sistema**. Entre la información disponible se encuentra la versión de firmware, la dirección IP, los ajustes de red y de seguridad, los ajustes de eventos y los elementos recientes del registro.

Registros e informes

La página **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports (Configuración > Configuración de controlador adicional > Opciones del sistema > Soporte > Registros e informes)** genera registros e informes de utilidad para análisis y resolución de problemas del sistema. Si se pone en contacto con el soporte técnico de Axis, incluya un Informe del sistema junto con su consulta.

Registro del sistema – Proporciona información sobre eventos del sistema.

Registro de acceso – Enumera todos los intentos fallidos de acceder al producto. También se puede configurar el registro de acceso para obtener una lista de todas las conexiones al producto (consulte a continuación).

Ver informe del servidor – Proporciona información acerca del estado del producto en una ventana emergente. El registro de acceso se incluye automáticamente en el informe del servidor.

Descargar el informe del servidor – Crea un archivo .zip que incluye un archivo de texto en formato UTF–8 con un informe completo del servidor. Seleccione la opción **Incluir captura desde visualización en directo** para incluir una instantánea de la visualización en directo del producto. El archivo .zip debe adjuntarse siempre que se contacte con el servicio técnico.

Lista de parámetros – Muestra los parámetros del producto y su configuración actual. Puede resultar útil para solucionar problemas o al ponerse en contacto con el servicio técnico de Axis.

Lista de conexiones – Enumera a todos los clientes que están accediendo actualmente a transmisiones de medios.

Informe de fallos – Genera un archivo con la información de depuración. El informe tarda varios minutos en generarse.

Los niveles de registro para los registros del sistema y de acceso se configuran en **Setup > Additional Controller Configuration > System Options > Support > Logs & Reports > Configuration (Configuración > Configuración del controlador adicional > Opciones del sistema > Soporte > Informes y registros > Configuración)**. El registro de acceso se puede configurar para obtener una lista de todas las conexiones al producto (seleccione Críticas, advertencias e información).

Avanzada

Secuencias de comandos

Las secuencias de comandos permiten a los usuarios experimentados personalizar y utilizar sus propias secuencias de comandos.

AVISO

Un uso incorrecto puede causar comportamientos inesperados y pérdida de contacto con el producto de Axis.

Axis recomienda encarecidamente no utilizar esta función, a menos que se comprendan las consecuencias. El servicio técnico de Axis no proporciona asistencia para problemas relacionados con secuencias de comandos personalizadas.

Para abrir el editor de secuencias de comandos, vaya a **Setup > Additional Controller Configuration > System Options > Advanced > Scripting (Configuración > Configuración de controlador adicional > Opciones del sistema > Avanzadas > Secuencias de comandos)**. Si una secuencia de comandos causa problemas, restablezca el producto a su configuración predeterminada de fábrica; consulte *page 38*.

Para obtener más información, visite *www.axis.com/developer*.

Carga de archivos

Se pueden cargar archivos, como páginas web e imágenes, en el producto de Axis y utilizarlos como ajustes personalizados. Para cargar un archivo, vaya a **Setup (Configuración) > Additional Controller Configuration (Configuración adicional del controlador) > System Options (Opciones del sistema) > Advanced (Avanzadas) > File Upload (Cargar archivos)**.

Se puede acceder a los archivos cargados en `http://<ip address>/local/<user>/<file name>`, donde `<user>` es el grupo de usuarios seleccionado (administrador) para el archivo cargado.

Localización de problemas

Restablezca la configuración predeterminada de fábrica

Importante

Hay que valorar bien es necesario restablecer la configuración predeterminada de fábrica. Todos los valores, incluida la dirección IP, se restablecerán a la configuración predeterminada de fábrica.

Para restablecer el producto a la configuración predeterminada de fábrica:

1. Desconecte la alimentación del producto.
2. Mantenga pulsado el botón de control mientras vuelve a conectar la alimentación. Consulte *Guía de productos, on page 6*.
3. Mantenga pulsado el botón de control durante 25 segundos hasta que el indicador LED de estado se ponga en ámbar por segunda vez.
4. Suelte el botón de control. El proceso finalizará cuando el indicador LED de estado se ilumine en color verde. El producto se ha restablecido a la configuración predeterminada de fábrica. Si no hay ningún servidor DHCP disponible en la red, la dirección IP predeterminada será `192.168.0.90`.
5. Utilice las herramientas del software de instalación y gestión para asignar una dirección IP, configurar la contraseña y acceder al producto.

También es posible restablecer los parámetros a los valores predeterminados de fábrica mediante la interfaz web. Vaya a (Ajustes > Sistema >Mantenimiento) (Preferencias > Configuración del dispositivo adicional > Opciones del sistema > Mantenimiento) **Setup > Additional Controller Configuration > Setup > System Options > Maintenance** (Configuración > Configuración del dispositivo adicional > Opciones del sistema > Opciones del sistema > Mantenimiento) y haga clic en **Default (Predeterminado)**.

Cómo comprobar el firmware actual

El firmware es un tipo de software que determina la funcionalidad de los dispositivos de red. Una de las acciones que deberá llevar a cabo en primer lugar a la hora de solucionar problemas será comprobar la versión actual del firmware. La versión más reciente podría contener una corrección que solucione su problema concreto.

La versión de firmware actual instalada en el producto de Axis se muestra en la página de vista general.

Cómo actualizar el firmware

Importante

- Su distribuidor se reserva el derecho de realizar cobros por cualquier reparación relativa a una actualización incorrectamente realizada por el usuario.
- Al actualizar el firmware se guarda la configuración preconfigurada y personalizada (en caso de que esta función esté disponible en el firmware), si bien Axis Communications AB no puede garantizarlo.
- Si instala una versión de firmware anterior, a continuación deberá restablecer el producto a la configuración predeterminada de fábrica.

Nota

- Una vez finalizado el proceso de actualización, el producto se reinicia automáticamente. Si reinicia manualmente el producto después de la actualización, espere 5 minutos, incluso si sospecha que la actualización ha fallado.
- Puesto que la base de datos de usuarios, grupos, credenciales y otros datos se actualiza con la actualización del firmware, el primer inicio podría tardar unos minutos en completarse. El tiempo necesario dependerá de la cantidad de datos.
- Al actualizar el producto de Axis con el firmware más reciente, el producto obtiene las últimas funciones disponibles. Lea siempre las instrucciones de actualización y las notas de versión disponibles en cada nueva versión antes de actualizar el firmware.

1. Descargue a su ordenador el último archivo de firmware, disponible de forma gratuita en *www.axis.com/support*
2. Acceda a **Setup > Additional Controller Configuration > System Options > Maintenance (Configuración > Configuración de controlador adicional > Opciones del sistema > Mantenimiento)** en la página web del producto.
3. Bajo **Upgrade Server (Actualizar servidor)**, haga clic en **Choose file (Elegir archivo)** y localice el archivo en su equipo.
4. Si desea que el producto se restablezca automáticamente a los ajustes predeterminados de fábrica, al terminar la actualización marque la casilla de verificación **Default (Predeterminada)**.
5. Haga clic en **Actualizar**.
6. Espere alrededor de 5 minutos a que el producto se actualice y se reinicie. A continuación, borre la caché del navegador.
7. Acceder al producto.

Síntomas, posibles causas y soluciones

Problemas al actualizar el firmware

Error durante la actualización del firmware	Cuando se produce un error en la actualización del firmware, el producto vuelve a cargar el firmware anterior. Compruebe el archivo de firmware e inténtelo de nuevo.

Problemas al configurar la dirección IP

Al utilizar ARP/Ping	Vuelva a intentar la instalación. La dirección IP debe establecerse durante un intervalo de dos minutos desde que se proporciona alimentación eléctrica al producto. Asegúrese de que la longitud de Ping esté ajustada a 408. Para obtener instrucciones, consulte la Guía de instalación en la página correspondiente del producto en *axis.com*.
El producto se encuentra en una subred distinta	Si la dirección IP prevista para el producto y la dirección IP del ordenador utilizado para acceder al producto se encuentran en subredes distintas, no se podrá configurar la dirección IP. Póngase en contacto con el administrador de red para obtener una dirección IP.
La dirección IP ya la utiliza otro dispositivo	Desconecte el producto de Axis de la red. Ejecute el comando "Ping" (en una ventana de comando/DOS, escriba `ping` y la dirección IP del producto): • Si recibe: `Reply from <IP address>: bytes=32; time=10...`, significará que la dirección IP podría estar en uso por otro dispositivo de la red. Solicite una nueva dirección IP al administrador de red y vuelva a instalar el producto. • Si recibe lo siguiente: `Request timed out`, significa que la dirección IP está disponible para su uso con el producto Axis. Compruebe el cableado y vuelva a instalar el producto.
Posible conflicto de dirección IP con otro dispositivo de la misma subred	Se utiliza la dirección IP estática del producto de Axis antes de que el servidor DHCP configure una dirección dinámica. Esto significa que, si otro dispositivo utiliza la misma dirección IP estática predeterminada, podría haber problemas para acceder al producto.

No se puede acceder al producto desde un navegador

No se puede iniciar sesión	Cuando HTTPS esté activado, asegúrese de que se utiliza el protocolo correcto (HTTP o HTTPS) al intentar iniciar sesión. Puede que tenga que escribir manualmente `http` o `https` en el campo de dirección del navegador.

	Si se pierde la contraseña del directorio raíz del usuario, habrá que restablecer el producto a su configuración predeterminada de fábrica. Consulte *Restablezca la configuración predeterminada de fábrica, on page 38*.
El servidor DHCP ha cambiado la dirección IP	Las direcciones IP obtenidas de un servidor DHCP son dinámicas y pueden cambiar. Si la dirección IP ha cambiado, acceda a la utilidad AXIS IP Utility o AXIS Device Manager para localizar el producto en la red. Identifique el producto utilizando el modelo o el número de serie, o por su nombre de DNS (si se ha configurado el nombre). Si es necesario, se puede asignar una dirección IP estática manualmente. Para obtener instrucciones, consulte el documento Cómo asignar una dirección IP y acceder al dispositivo en la página de producto en *axis.com*
Error de certificado cuando se utiliza IEEE 802.1X	Para que la autentificación funcione correctamente, la configuración de fecha y hora del producto de Axis se debe sincronizar con un servidor NTP. Consulte .

Se puede acceder al producto localmente pero no externamente

Configuración del router	Para configurar el router a fin de permitir el tráfico de datos entrantes al producto Axis, active la función de NAT transversal, que tratará de configurar automáticamente el router para permitir el acceso al producto Axis, consulte *NAT transversal (asignación de puertos) para IPv4, on page 33*. El router debe admitir UPnP®.
Protección de firewall	Pida al administrador de red que compruebe el firewall de Internet.
Se requieren routers predeterminados	Compruebe si debe configurar el router en **Setup > Network Settings (Configuración > Ajustes de red)** o **Setup > Additional Controller Configuration > System Options > Network > TCP/IP > Basic (Configuración > Configuración de controlador adicional > Opciones del sistema > Red > TCP/IP > Básica)**.

Especificaciones

El texto marcado **UL** solo es válido para instalaciones UL 293 o UL 294.

Indicadores LED

LED	Color	Indicación
Red	Verde	Fijo para indicar una conexión a una red de 100 MBits/s. Parpadea para indicar actividad en la red.
	Ámbar;	Fijo para indicar una conexión a una red de 10 MBits/s. Parpadea para indicar actividad en la red.
	Apagado	No hay conexión a la red.
Estado	Verde	Fijo para indicar un funcionamiento normal.
	Ámbar;	Fijo durante el inicio y al restaurar valores de configuración.
	Rojo	Parpadea despacio si se ha producido un error en una actualización.
Alimentación	Verde	Funcionamiento normal.
	Ámbar;	Parpadea en verde/ámbar durante la actualización del firmware.
Sobrecorriente de relé	Rojo	Fijo con cortocircuito o si se ha detectado sobretensión.
	Apagado	Funcionamiento normal.
Sobrecorriente del lector	Rojo	Fijo con cortocircuito o si se ha detectado sobretensión.
	Apagado	Funcionamiento normal.
Relé	Verde	Relé activo.[2]
	Apagado	Relé inactivo.

Nota

- Se puede configurar el LED de estado para que parpadee mientras haya un evento activo.
- Se puede configurar el LED de estado para que parpadee e identifique la unidad. Acceda a **Setup > Additional Controller Configuration > System Options > Maintenance (Configuración > Configuración del controlador adicional > Opciones del sistema > Mantenimiento)**.

Botones

Botón de control

El botón de control se utiliza para lo siguiente:

- Restablecer el producto a la configuración predeterminada de fábrica. Consulte *Restablezca la configuración predeterminada de fábrica, on page 38*.

Conectores

Conector de red

Conector Ethernet RJ45 con alimentación a través de Ethernet Plus (PoE+).

UL: La alimentación a través de Ethernet (PoE) se debe suministrar mediante un inyector de alimentación a través de Ethernet IEEE 802.3af/802.3at Tipo 1, Clase 3, o de alimentación a través de Ethernet Plus (PoE +) IEEE

2. El relé está activo cuando COM está conectado a NO.

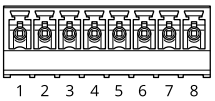
802.3 at Tipo 2 Clase 4 incluidos en la lista UL 294 que ofrezca 44–57 V CC, 15,4 W / 30 W. La alimentación a través de Ethernet (PoE) se ha evaluado conforme a UL con AXIS T8133 Midspan 30 W 1 puerto.

Conector de lector

Dos bloques de terminales de 8 pines, ambos compatibles con los protocolos RS485 y Wiegand para la comunicación con el lector.

Los valores especificados de salida de potencia se comparten entre los dos puertos de lector. Esto significa que se reservan 486 mA a 12 V CC para todos los lectores conectados al controlador de puerta.

Seleccione el protocolo que desea utilizar en la página web del producto.



Configurado para RS485

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Proporciona alimentación al lector.	12 V CC, máx. 486 mA combinados para ambos lectores
RX/TX	3-4	Full-duplex: RX. Semidúplex: RX/TX.	
TX	5–6	Full-duplex: TX.	
Configurable (entrada o salida)	7–8	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	0 a máx. 30 V CC
		Salida digital: Si se utiliza con una carga inductiva, como un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a 30 V CC máx., colector abierto, 100 mA

Importante

- Cuando el controlador alimenta el lector, la longitud de cable cualificada es de hasta 200 m (656 ft).
- Si el controlador no alimenta el lector, la longitud de cable cualificada para datos del lector es de hasta 1000 m (3280,8 ft) si se cumplen los siguientes requisitos de cable: 1 par trenzado con blindaje AWG 24, impedancia 120 ohm.

Configurado para Wiegand

Función	Pin	Nota	Especificaciones
Tierra CC (GND)	1		0 V CC
Salida de CC (+12 V)	2	Proporciona alimentación al lector.	12 V CC, máx. 486 mA combinados para ambos lectores

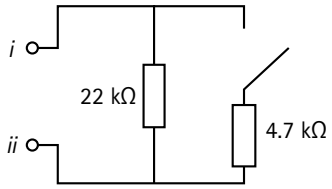
D0	3		
D1	4		
O	5–6	Salida digital, colector abierto	
Configurable (entrada o salida)	7–8	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	0 a máx. 30 V CC
		Salida digital: Si se utiliza con una carga inductiva, como un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a 30 V CC máx., colector abierto, 100 mA

Importante

- Cuando el controlador alimenta el lector, la longitud de cable cualificada es de hasta 150 m.
- Si el controlador no alimenta el lector, la longitud de cable cualificada para datos del lector es de hasta 150 m si se cumple el siguiente requisito de cable: AWG 22.

Entradas con supervisión

Para usar entradas supervisadas, instale resistencias de final de línea según el siguiente diagrama.



i Entrada

ii 0 V CC (-)

UL: Las entradas supervisadas no se han evaluado conforme UL para el uso de una alarma antirrobo. Solo el monitor de puerta y REX admiten supervisión con resistencias de final de línea.

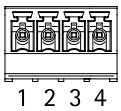
Nota

Se recomienda el uso de cables trenzados y blindados. Conecte el blindaje a 0 V CC.

Conector de puerta

Dos bloques de terminales de 4 pines para dispositivos de monitor de puerta (entrada digital).

El monitor de puerta admite supervisión con resistencias de final de línea. Si se interrumpe la conexión, se activa una alarma. Para utilizar entradas con supervisión, debe instalar resistencias de fin de línea. Use el diagrama de conexión para las entradas supervisadas. Consulte .



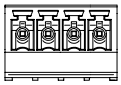
Función	Pin	Notas	Especificaciones
Tierra CC	1, 3		0 V CC
Entrada	2, 4	Para la comunicación con el monitor de la puerta. Entrada digital o entrada supervisada: conéctela al pin 1 o 3 respectivamente para activarla, o déjela flotando (desconectada) para desactivarla.	De 0 a 30 V CC máx.

Importante

La longitud de cable cualificada es de hasta 200 m (656 pies) si se cumplen los siguientes requisitos de cable: AWG 24.

Conector de relé

Dos bloques de terminales de 4 pines para relés de forma de contacto C que se pueden utilizar, por ejemplo, para controlar una cerradura o una interfaz para una puerta.



Función	Pin	Notas	Especificaciones
Tierra CC (GND)	1		0 V CC
NO	2	Normalmente abierto. Para conectar dispositivos de relés. Conecte un bloqueo de seguridad negativa entre NO y masa CC. Los dos pines de relé se separan de forma galvanizada del resto del circuito si no se utilizan puentes.	Corriente máxima = 2 A por relé Voltaje máx. = 30 V CC
COM	3	Común	
NC	4	Normalmente cerrado. Para conectar dispositivos de relés. Conecte un bloqueo de seguridad negativa entre NC y masa CC. Los dos pines de relé se separan de forma galvanizada del resto del circuito si no se utilizan puentes.	

Puente de alimentación de relé

Cuando el puente de alimentación de relé está colocado, conecta 12 V CC o 24 V CC al pin COM del relé.

Se puede utilizar para conectar una cerradura entre los pines GND y NO, o GND y NC.

Fuente de alimentación	Potencia máxima a 12 V CC[3]	Potencia máxima a 24 V CC[3]
ENTRADA DE CC	1600 mA	800 mA
PoE	800 mA	400 mA

3. La alimentación se comparte entre los dos relés y E/S AUX 12 V CC.

AVISO

Si la cerradura no está polarizada, le recomendamos añadir un diodo de regreso externo.

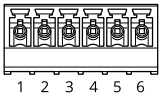
Conector auxiliar

Utilice el conector auxiliar con dispositivos externos, por ejemplo, en combinación con detección de movimiento, activación de eventos y notificaciones de alarma. Además del punto de referencia de 0 V CC y la alimentación (salida de CC), el conector auxiliar ofrece la interfaz para:

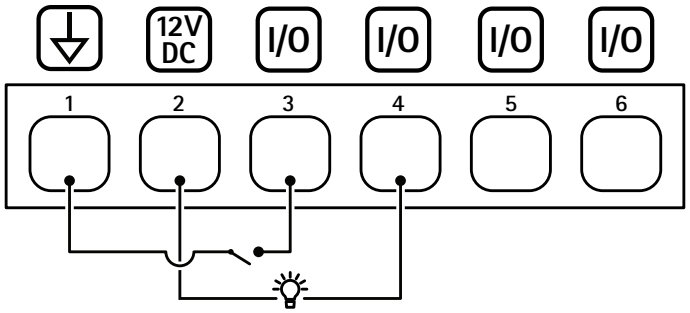
Entrada digital – Conectar dispositivos que puedan alternar entre circuitos cerrados y abiertos, por ejemplo, sensores PIR, contactos de puertas y ventanas o detectores de cristales rotos.

Salida digital – Conectar dispositivos externos como relés y LED. Los dispositivos conectados se pueden activar mediante la interfaz de programación de aplicaciones VAPIX® o desde la página web del producto.

Bloque de terminales de 6 pines



Función	Pin	Notas	Especificaciones
Tierra CC	1		0 V CC
Salida de CC	2	Se puede utilizar para alimentar equipos auxiliares. Nota: Este pin solo se puede utilizar como salida de alimentación.	12 V CC Carga máx. = 50 mA para cada E/S
Configurable (entrada o salida)	3–6	Entrada digital: conéctela al pin 1 para activarla, o bien déjela suelta (sin conectar) para desactivarla.	De 0 a 30 V CC máx.
		Salida digital: conectada internamente a pin 1 (tierra CC) cuando está activa, y suelta (desconectada) cuando está inactiva. Si se utiliza con una carga inductiva, por ejemplo, un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión. Cada E/S puede conducir una carga externa de 12 V CC, 50 mA (máx.), si se utiliza una salida interna de 12 V CC (pin 2). En caso de usar conexiones de colector abierto en combinación con una fuente de alimentación externa, las E/S pueden gestionar el suministro de CC de 0 – 30 V CC, 100 mA.	De 0 a 30 V CC máx., colector abierto, 100 mA

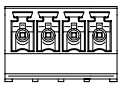


1 *Tierra CC*
2 *Salida de CC 12 V*
3 *E/S configurada como entrada*
4 *E/S configurada como salida*
5 *E/S configurable*
6 *E/S configurable*

Conector externo

Bloque de terminales de 4 pines para conectar dispositivos externos, como detectores de rotura de vidrio o de incendio.

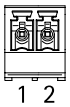
UL: El conector no ha sido evaluado conforme a UL para el uso de una alarma antirrobo/antiincendios.



Función	Pin	Notas	Especificaciones
Tierra CC	1, 3		0 V CC
Configurable (entrada o salida)	2, 4	Entrada digital: conéctela al pin 1 o 3 para activarla, o bien déjela suelta (desconectada) para desactivarla.	De 0 a 30 V CC máx.
		Salida digital: conéctela al pin 1 o 3 para activarla o bien déjela suelta (desconectada) para desactivarla. Si se utiliza con una carga inductiva, por ejemplo, un relé, conecte un diodo en paralelo a la carga como protección contra transitorios de tensión.	De 0 a 30 V CC máx., colector abierto, 100 mA

Conector de alimentación

Bloque de terminales de 2 pines para la entrada de alimentación de CC. Use una fuente de alimentación limitada (LPS) que cumpla los requisitos de seguridad de baja tensión (SELV) con una potencia nominal de salida limitada a ≤100 W o una corriente nominal de salida limitada a ≤5 A.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1		0 V CC
Entrada CC	2	Para alimentar el controlador cuando no se use la alimentación a través de Ethernet. Nota: Este pin solo se puede utilizar como entrada de alimentación.	10,5–28 V CC, 36 W máx.

UL: Una fuente de alimentación UL 294, UL 293 o UL 603 debe suministrar la alimentación de CC, en función de la aplicación, con las clasificaciones adecuadas.

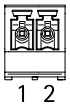
Conector de entrada de batería de reserva

Para una solución de reserva mediante una batería con cargador integrado. Entrada 12 V CC.

UL: El conector no ha sido evaluado conforme a UL.

Importante

Cuando se utiliza la entrada de batería, se debe conectar en serie un fusible de fusión lenta externo de 3 A.



Función	Pin	Notas	Especificaciones
0 V CC (-)	1		0 V CC
Entrada de batería	2	Para alimentar el controlador de puerta cuando no hay otras fuentes de alimentación disponibles. Nota: Este pin solo se puede utilizar como entrada de alimentación de batería. Solo para la conexión con SAI.	11 – 13,7 V CC, máx. 36 W

Información de seguridad

Niveles de peligro

⚠ PELIGRO
Indica una situación peligrosa que, si no se evita, provocará lesiones graves o la muerte.

⚠ ADVERTENCIA
Indica una situación peligrosa que, si no se evita, puede provocar lesiones graves o la muerte.

⚠ PRECAUCIÓN
Indica una situación peligrosa que, si no se evita, puede provocar lesiones moderadas o leves.

AVISO
Indica una situación peligrosa que, si no se evita, puede provocar daños materiales.

Otros niveles de mensaje

Importante
Indica información importante que es fundamental para que el producto funcione correctamente.

Nota
Indica información útil que ayuda a aprovechar el producto al máximo.

Interfaz web

Nota

Esta sección solo es válida para AXIS A1601 Network Door Controller con AXIS Camera Station Secure Entry firmware.

: Cambie entre **Device settings** (Ajustes del dispositivo) y la información general de **Analytics** (Analíticas).

: Mostrar u ocultar el menú principal.

Help (Ayuda): Acceda a la ayuda del producto, a las notas de la versión y a la guía del ciclo de vida.

Information (Información):

- **About (Acerca de)**: Puede consultar la información del dispositivo, como la versión de AXIS OS y el número de serie.
- **Legal (Aviso legal)**: Lea información sobre cookies y licencias.
- **Feedback (Comentarios)**: Puede enviarnos comentarios para ayudarnos a mejorar su experiencia de usuario.
- **Analytics data (Datos de analíticas)**: Puede compartir datos no personales del navegador.
- **Device server report (Informe del servidor del dispositivo)**: Download the device server report (Descargar informe del servidor del dispositivo).

Administrador:

- : Información sobre el usuario que ha iniciado sesión.
- : Cambiar el idioma.
- : Definir un tema claro o un tema oscuro.
- **Change account (Cambiar cuenta)**: Cierre sesión en la cuenta actual e inicie sesión en una cuenta nueva.
- **Cerrar sesión**: Cierre sesión en la cuenta actual.

Estado

Estado de sincronización de hora

Muestra la información de sincronización de NTP, como si el dispositivo está sincronizado con un servidor NTP y el tiempo que queda hasta la siguiente sincronización, así como el estado del PTP.

Configuración de NTP: Ver y actualizar los ajustes de NTP. Le lleva a la página **Time and location (Hora y localización)**, donde puede cambiar los ajustes de NTP.

Información sobre el dispositivo

Muestra información sobre el dispositivo, como la versión del AXIS OS y el número de serie.

Actualización de AXIS OS: Actualizar el software en el dispositivo. Le lleva a la página de mantenimiento donde puede realizar la actualización.

Dispositivo

Alarmas

Device motion (Movimiento del dispositivo): Active esta opción para desencadenar una alarma en el sistema cuando se detecte un movimiento del dispositivo.

Casing open (Apertura de carcasa): Active esta opción para desencadenar una alarma en el sistema cuando se detecte una carcasa del controlador de puerta abierta. Desactive este ajuste para los controladores de puerta básicos.

External tamper (Manipulación externa): Con esta opción se desencadena una alarma en el sistema si se detecta una manipulación externa. Por ejemplo, cuando alguien abre o cierra el armario externo.

- **Normal state (Estado normal)**: Haga clic en  para circuito abierto y en  para circuito cerrado.
- **Supervised input (Entrada supervisada)**: Active la supervisión del estado de entrada y configure las resistencias de final de línea.
  - Para utilizar la primera conexión paralela, seleccione **Parallel first connection with a 22 KΩ parallel resistor and a 4.7 KΩ serial resistor (Primera conexión en paralelo con una resistencia de 22 KΩ en paralelo y una resistencia de 4,7 KΩ en serie)**.
  - Para utilizar la primera conexión en serie, seleccione **Serial first connection (Primera conexión en serie)** y seleccione los valores de la resistencia en la lista desplegable **Resistor values (Valores de resistencia)**.

Periféricos

Lectores

Add (agregar) : Haga clic aquí para añadir un lector.

Axis network readers (Lectores de red Axis): Puede añadir al controlador hasta 16 lectores Bluetooth, sin necesidad de licencia.

- **Name (Nombre)**: Introduzca el nombre del lector.
- **Lector**: Seleccione un lector de la lista desplegable.
- **IP address (Dirección IP)**: Introduzca la dirección IP del lector manualmente.
- **Nombre de usuario**: Introduzca el nombre de usuario del lector.
- **Contraseña**: Introduzca la contraseña de usuario del lector.
- **Ignore server certificate verification (Ignorar verificación de certificado de servidor)**: Active esta opción para ignorar la verificación.
- **I/O ports and relays (Puertos de E/S y relés)**: Expanda para configurar los puertos de E/S y relés.
  - **Port (Puerto)**: Muestra el nombre del puerto.
  - **Direction (Dirección)**: Indica que se trata de un puerto de entrada o salida.
  - **Normal state (Estado normal)**: Haga clic en  para circuito abierto y en  para circuito cerrado.

Axis network intercoms (es preciso volver a configurarlos en AXIS Camera Station)

- **Name (Nombre)**: Introduzca el nombre del lector.
- **Lector**: Seleccione un lector de la lista desplegable.
- **IP address (Dirección IP)**: Introduzca la dirección IP del lector manualmente.
- **Nombre de usuario**: Introduzca el nombre de usuario del lector.
- **Contraseña**: Introduzca la contraseña de usuario del lector.
- **Ignore server certificate verification (Ignorar verificación de certificado de servidor)**: Active esta opción para ignorar la verificación.

AXIS License Plate Verifier (es preciso volver a configurarlo en AXIS Camera Station)

- **Name (Nombre)**: Introduzca el nombre del lector.
- **API key (Clave API)**: Introduzca la clave API.
- **Generate (Generar)**: Haga clic para generar la clave API.
- **Copy API-key (Copiar la clave API)**: Haga clic para copiar la clave API y guárdela en un lugar seguro.

AXIS Barcode Reader (es preciso volver a configurarlo en AXIS Camera Station)

- **Name (Nombre)**: Introduzca el nombre del lector.
- **API key (Clave API)**: Introduzca la clave API.
- **Generate (Generar)**: Haga clic para generar la clave API.
- **Copy API-key (Copiar la clave API)**: Haga clic para copiar la clave API y guárdela en un lugar seguro.

Editar: Seleccione un lector y haga clic en **Edit (Editar)** para realizar cambios en el lector seleccionado.

Eliminar: Seleccione los lectores y haga clic en **Delete (Eliminar)** para eliminar los lectores seleccionados.

Cerraduras inalámbricas

Puede conectar hasta 16 bloqueos inalámbricos ASSA ABLOY Aperio mediante el AH30 Communication Hub. El bloqueo inalámbrico requiere licencia.

Nota

Debe instalar AH30 Communication Hub en el lado seguro.

Conectar concentrador de comunicaciones: Haga clic para conectar los bloqueos inalámbricos.

Actualizar

Actualizar lectores: Haga clic para actualizar el software del lector. Solo puede actualizar los lectores compatibles cuando estén en línea.

Upgrade converters (Actualizar convertidores): Haga clic para actualizar el software del convertidor. Solo puede actualizar los convertidores compatibles cuando estén en línea.

Sistema

Hora y ubicación

Fecha y hora

El formato de fecha y hora depende de la configuración de idioma del navegador web.

Nota

Es aconsejable sincronizar la fecha y hora del dispositivo con un servidor NTP.

Synchronization (Sincronización): Seleccione una opción para la sincronización de la fecha y la hora del dispositivo.

- **Automatic date and time (Fecha y hora automáticos) (PTP)**: Sincronice mediante el protocolo de tiempo de precisión.
- **Fecha y hora automáticas (servidores NTS KE manuales)**: Sincronice con los servidores de establecimiento de claves NTP seguros conectados al servidor DHCP.
  - **Servidores NTS KE manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Trusted NTS KE CA certificates (Certificados CA de NTS KE de confianza)**: Seleccione los certificados CA de confianza que se usarán para la sincronización horaria segura de NTS KE o no seleccione ninguno.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (los servidores NTP utilizan DHCP)**: Se sincroniza con los servidores NTP conectados al servidor DHCP.
  - **Servidores NTP alternativos**: Introduzca la dirección IP de un servidor alternativo o de dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Fecha y hora automáticas (servidores NTP manuales)**: Se sincroniza con los servidores NTP que seleccione.
  - **Servidores NTP manuales**: Introduzca la dirección IP de un servidor NTP o de dos. Si usa dos servidores NTP, el dispositivo sincroniza y adapta la fecha y hora en función de la información de los dos.
  - **Tiempo máximo de encuesta NTP**: Seleccione la cantidad máxima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
  - **Tiempo mínimo de encuesta NTP**: Seleccione la cantidad mínima de tiempo que debe esperar el dispositivo antes de que sondee el servidor NTP para obtener una hora actualizada.
- **Custom date and time (Personalizar fecha y hora)**: Establezca manualmente la fecha y hora. Haga clic en **Get from system (Obtener del sistema)** para obtener una vez la configuración de fecha y hora desde su ordenador o dispositivo móvil.

Time zone (Zona horaria): Seleccione la zona horaria que desee utilizar. La hora se ajustará automáticamente para el horario de verano y el estándar.

- **DHCP**: Adopta la zona horaria del servidor DHCP. El dispositivo debe estar conectado a un servidor DHCP (v4 o v6) para poder seleccionar esta opción. Si ambas versiones están disponibles, el dispositivo prefiere las zonas horarias IANA antes que POSIX, y DHCPv4 a DHCPv6.
  - DHCPv4 utiliza la opción 100 para las zonas horarias POSIX y la opción 101 para las zonas horarias IANA.
  - DHCPv6 utiliza la opción 41 para POSIX y la opción 42 para IANA.
- **Manual**: Seleccione una zona horaria de la lista desplegable.

Nota

El sistema utiliza los ajustes de fecha y hora en todas las grabaciones, registros y ajustes del sistema.

Time sync status (Estado de sincronización de hora): Muestra información de sincronización NTP y de estado del PTP.

Network time synchronized capture (Captura sincronizada con la hora de red): Active esta opción para permitir que varias cámaras capten imágenes simultáneamente.

Red

Red

IPv4

Asignar IPv4 automáticamente: Seleccione IPv4 IP automática (DHCP) para permitir que la red asigne automáticamente su dirección IP, máscara de subred y router, sin configuración manual. Recomendamos utilizar la asignación automática de IP (DHCP) para la mayoría de las redes.

IP address (Dirección IP): Introduzca una dirección IP única para el dispositivo. Las direcciones IP estáticas se pueden asignar de manera aleatoria dentro de redes aisladas, siempre que cada dirección asignada sea única. Para evitar conflictos, le recomendamos ponerse en contacto con el administrador de la red antes de asignar una dirección IP estática.

Subnet mask (Máscara de subred): Introduzca la máscara de subred para definir qué direcciones se encuentran dentro de la red de área local. Cualquier dirección fuera de la red de área local pasa por el router.

Router: Introduzca la dirección IP del router predeterminado (puerta de enlace) utilizada para conectar dispositivos conectados a distintas redes y segmentos de red.

Volver a la dirección IP estática si DHCP no está disponible: Seleccione si desea agregar una dirección IP estática para utilizarla como alternativa si DHCP no está disponible y no puede asignar una dirección IP automáticamente.

Nota

Si DHCP no está disponible y el dispositivo utiliza una reserva de dirección estática, la dirección estática se configura con un ámbito limitado.

IPv6

Assign IPv6 automatically (Asignar IPv6 automáticamente): Seleccione esta opción para activar IPv6 y permitir que el router de red asigne automáticamente una dirección IP al dispositivo.

Nombre de host

Asignar nombre de host automáticamente: Seleccione esta opción para que el router de red asigne automáticamente un nombre de host al dispositivo.

Hostname (Nombre de host): Introduzca el nombre de host manualmente para usarlo como una forma alternativa de acceder al dispositivo. El informe del servidor y el registro del sistema utilizan el nombre de host. Los caracteres permitidos son A–Z, a–z, 0–9 y -.

Active las actualizaciones de DNS dinámicas: Permite que el dispositivo actualice automáticamente los registros de su servidor de nombres de dominio cada vez que cambie la dirección IP del mismo.

Register DNS name (Registrar nombre de DNS): Introduzca un nombre de dominio único que apunte a la dirección IP de su dispositivo. Los caracteres permitidos son A–Z, a–z, 0–9 y -.

TTL: El tiempo de vida (Time to Live, TTL) establece cuánto tiempo permanece válido un registro DNS antes de que sea necesario actualizarlo.

Servidores DNS

Asignar DNS automáticamente: Seleccione esta opción para permitir que el servidor DHCP asigne dominios de búsqueda y direcciones de servidor DNS al dispositivo automáticamente. Recomendamos DNS automática (DHCP) para la mayoría de las redes.

Search domains (Dominios de búsqueda): Si utiliza un nombre de host que no esté completamente cualificado, haga clic en **Add search domain (Agregar dominio de búsqueda)** y escriba un dominio en el que se buscará el nombre de host que usa el dispositivo.

DNS servers (Servidores DNS): Haga clic en **Agregar servidor DNS** e introduzca la dirección IP del servidor DNS. Este servidor proporciona la traducción de nombres de host a las direcciones IP de su red.

Nota

Si DHCP está deshabilitado, las funciones que dependen de la configuración automática de la red, como el nombre de host, los servidores DNS, NTP y otras, podrían dejar de funcionar.

HTTP y HTTPS

HTTPS es un protocolo que proporciona cifrado para las solicitudes de página de los usuarios y para las páginas devueltas por el servidor web. El intercambio de información cifrado se rige por el uso de un certificado HTTPS, que garantiza la autenticidad del servidor.

Para utilizar HTTPS en el dispositivo, debe instalar un certificado HTTPS. Vaya a **System > Security (Sistema > Seguridad)** para crear e instalar certificados.

Allow access through (Permitir acceso mediante): Seleccione si un usuario tiene permiso para conectarse al dispositivo a través de **HTTP**, **HTTPS** o ambos protocolos **HTTP and HTTPS (HTTP y HTTPS)**.

Nota

Si visualiza páginas web cifradas a través de HTTPS, es posible que experimente un descenso del rendimiento, especialmente si solicita una página por primera vez.

HTTP Port (Puerto HTTP): Especifique el puerto HTTP que se utilizará. El dispositivo permite el puerto 80 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

HTTPS Port (Puerto HTTPS): Especifique el puerto HTTPS que se utilizará. El dispositivo permite el puerto 443 o cualquier puerto en el rango 1024-65535. Si ha iniciado sesión como administrador, también puede introducir cualquier puerto en el rango 1-1023. Si utiliza un puerto en este rango, recibirá una advertencia.

Certificado: Seleccione un certificado para habilitar HTTPS para el dispositivo.

Protocolos de detección de red

Bonjour®: Seleccione esta opción para permitir la detección automática en la red.

Nombre de Bonjour: Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

UPnP®: Seleccione esta opción para permitir la detección automática en la red.

Nombre de UPnP: Introduzca un nombre descriptivo; será el que se muestre en la red. El nombre predeterminado es el nombre del dispositivo seguido de la dirección MAC.

WS-Discovery: Seleccione esta opción para permitir la detección automática en la red.

LLDP y CDP: Seleccione esta opción para permitir la detección automática en la red. No permitir los protocolos LLDP y CDP podría afectar a la negociación PoE. Para solucionar cualquier problema con la negociación de alimentación PoE, configure el switch PoE solo para la negociación de alimentación PoE del hardware.

Neighbors (Contadores contiguos): Haga clic para mostrar información sobre dispositivos próximos conectados a la misma red.

Conexión a la nube con un clic

La conexión One-Click Cloud (O3C), junto con un servicio O3C, ofrece acceso seguro y sencillo a Internet para acceder al vídeo en directo o grabado desde cualquier ubicación. Para obtener más información, consulte *axis.com/end-to-end-solutions/hosted-services*.

Allow O3C (Permitir O3C):

- **Un clic**: Esta es la opción predeterminada. Presione el botón de control del dispositivo para conectarse a O3C. Según el modelo del dispositivo, mantenga pulsado o pulse y suelte el botón hasta que el LED de estado parpadee. Registre el dispositivo en el servicio O3C en un plazo de 24 horas para activar la opción **Siempre** y mantenerse conectado. Si no lo registra, el dispositivo se desconectará de O3C.
- **Siempre**: El dispositivo intenta conectarse continuamente a un servicio O3C a través de Internet. Una vez registrado el dispositivo, permanece conectado. Utilice esta opción si el botón de control está fuera de su alcance.
- **No**: Desconecta el servicio O3C.

Proxy settings (Configuración proxy): Si es necesario, escriba los ajustes del proxy para conectarse al servidor proxy.

Host: Introduzca la dirección del servidor proxy.

Port (Puerto): Introduzca el número de puerto utilizado para acceder.

Inicio de sesión y **Contraseña**: En caso necesario, escriba un nombre de usuario y la contraseña del servidor proxy.

Authentication method (Método de autentificación):

- **Básico**: Este método es el esquema de autenticación más compatible con HTTP. Es menos seguro que el método **Digest** porque envía el nombre de usuario y la contraseña sin cifrar al servidor.
- **Digest**: Este método de autenticación es más seguro porque siempre transfiere la contraseña cifrada a través de la red.
- **Automático**: Esta opción permite que el dispositivo seleccione el método de autenticación automáticamente en función de los métodos admitidos. Da prioridad al método **Digest** por delante del **Básico**.

Owner authentication key (OAK) (Clave de autenticación de propietario [OAK]): Haga clic en **Get key (Obtener clave)** para obtener la clave de autenticación del propietario. Esto solo es posible si el dispositivo está conectado a Internet sin un cortafuegos o proxy.

SNMP

El protocolo de administración de red simple (SNMP) permite gestionar dispositivos de red de manera remota.

SNMP: Seleccione la versión de SNMP a usar.

- **v1 and v2c (v1 y v2c)**:
  - **Read community (Comunidad de lectura)**: Introduzca el nombre de la comunidad que tiene acceso de solo lectura a todos los objetos SNMP compatibles. El valor predeterminado es **público**.
  - **Write community (Comunidad de escritura)**: Escriba el nombre de la comunidad que tiene acceso de lectura o escritura a todos los objetos SNMP compatibles (excepto los objetos de solo lectura). El valor predeterminado es **escritura**.
  - **Activate traps (Activar traps)**: Active esta opción para activar el informe de trap. El dispositivo utiliza traps para enviar mensajes al sistema de gestión sobre eventos importantes o cambios de estado. En la interfaz web puede configurar traps para SNMP v1 y v2c. Las traps se desactivan automáticamente si cambia a SNMP v3 o desactiva SNMP. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Trap address (Dirección trap)**: introduzca la dirección IP o el nombre de host del servidor de gestión.
  - **Trap community (Comunidad de trap)**: Introduzca la comunidad que se utilizará cuando el dispositivo envía un mensaje trap al sistema de gestión.
  - **Traps**:
    - **Cold start (Arranque en frío)**: Envía un mensaje trap cuando se inicia el dispositivo.
    - **Link up (Enlace hacia arriba)**: Envía un mensaje trap cuando un enlace cambia de abajo a arriba.
    - **Link down (Enlace abajo)**: Envía un mensaje trap cuando un enlace cambia de arriba a abajo.
    - **Authentication failed (Error de autentificación)**: Envía un mensaje trap cuando se produce un error de intento de autentificación.

Nota

Todas las traps Axis Video MIB se habilitan cuando se activan las traps SNMP v1 y v2c. Para obtener más información, consulte *AXIS OS Portal > SNMP*.

- **v3**: SNMP v3 es una versión más segura que ofrece cifrado y contraseñas seguras. Para utilizar SNMP v3, recomendamos activar HTTPS, ya que la contraseña se envía a través de HTTPS. También evita que partes no autorizadas accedan a traps SNMP v1 y v2c sin cifrar. Si utiliza SNMP v3, puede configurar las traps a través de la aplicación de gestión de SNMP v3.
  - **Privacy (Privacidad)**: Seleccione el cifrado que desea usar para proteger sus datos SNMP.
  - **Password for the account "initial" (contraseña para la cuenta "Inicial")**: Introduzca la contraseña de SNMP para la cuenta denominada "Initial". Aunque la contraseña se puede enviar sin activar HTTPS, no lo recomendamos. La contraseña de SNMP v3 solo puede establecerse una vez, y preferiblemente solo cuando esté activado HTTPS. Una vez establecida la contraseña, dejará de mostrarse el campo de contraseña. Para volver a establecer la contraseña, debe restablecer el dispositivo a su configuración predeterminada de fábrica. Recuerde que la contraseña debe cumplir la política de contraseñas; consulte *Cuentas, on page 63*.

Clientes conectados

Muestra el número de conexiones y clientes conectados.

View details (Ver detalles): Consulte y actualice la lista de clientes conectados. La lista muestra la dirección IP, el protocolo, el puerto, el estado y PID/proceso de cada conexión.

Seguridad

Certificados

Los certificados se utilizan para autenticar los dispositivos de una red. Un dispositivo admite dos tipos de certificados:

- **Client/server certificates (Certificados de cliente/servidor)**
  Un certificado de cliente/servidor valida la identidad del dispositivo de Axis y puede firmarlo el propio dispositivo o emitirlo una autoridad de certificación (CA). Un certificado firmado por el propio producto ofrece protección limitada y se puede utilizar antes de que se obtenga un certificado emitido por una autoridad de certificación.
- **Certificados de autoridad de certificación**
  Puede utilizar un certificado de la autoridad de certificación (AC) para autenticar un certificado entre iguales, por ejemplo, para validar la identidad de un servidor de autentificación cuando el dispositivo se conecta a una red protegida por IEEE 802.1X. El dispositivo incluye varios certificados de autoridad de certificación preinstalados.

Se admiten estos formatos:

- Formatos de certificado: PEM, .CER y .PFX
- Formatos de clave privada: PKCS#1 y PKCS#12

Importante

Si restablece el dispositivo a los valores predeterminados de fábrica, se eliminarán todos los certificados. Los certificados CA preinstalados se vuelven a instalar.

Add certificate (Añadir certificado): Haga clic aquí para añadir un certificado. Se abre una guía paso a paso.

- **More (Más)** : Mostrar más campos que rellenar o seleccionar.
- **Almacenamiento de claves seguro**: Seleccione usar el **Trusted Execution Environment (SoC TEE)**, **Elemento seguro** o **Trusted Platform Module 2.0** para almacenar la clave privada de forma segura. Para obtener más información sobre el almacén de claves seguro que desea seleccionar, vaya a *help.axis.com/axis-os#cryptographic-support*.
- **Tipo de clave**: Seleccione la opción predeterminada o un algoritmo de cifrado diferente en la lista desplegable para proteger el certificado.

El menú contextual contiene:

- **Certificate information (Información del certificado)**: Muestra las propiedades de un certificado instalado.
- **Delete certificate (Eliminar certificado)**: Se elimina el certificado.
- **Create certificate signing request (Crear solicitud de firma de certificado)**: Se crea una solicitud de firma de certificado que se envía a una autoridad de registro para solicitar un certificado de identidad digital.

Almacenamiento de claves seguro:

- **Trusted Execution Environment (Entorno de ejecución fiable) (SoC TEE)**: Seleccione para usar SoC TEE para el almacén de claves seguro.
- **Secure element (Elemento seguro) (CC EAL 6+, FIPS 140-3 Nivel 3)**: Seleccione para utilizar un elemento seguro para un almacén de claves seguro.
- **Trusted Platform Module 2.0 (CC EAL4+, FIPS 140-2 nivel 2)**: Seleccione para usar TPM 2.0 para el almacén de claves seguro.

Control y cifrado de acceso a la red

IEEE 802.1x

IEEE 802.1x es un estándar IEEE para el control de admisión de red basada en puertos que proporciona una autentificación segura de los dispositivos de red conectados e inalámbricos. IEEE 802.1x se basa en el protocolo de autentificación extensible, EAP.

Para acceder a una red protegida por IEEE 802.1x, los dispositivos de red deben autenticarse ellos mismos. Un servidor de autentificación lleva a cabo la autentificación, normalmente un servidor RADIUS (por ejemplo, FreeRADIUS y Microsoft Internet Authentication Server).

IEEE 802.1AE MACsec

IEEE 802.1AE MACsec es un estándar IEEE para la seguridad del control de acceso a medios (MAC) que define la confidencialidad e integridad de los datos sin conexión para protocolos independientes de acceso a medios.

Certificados

Si se configura sin un certificado de la autoridad de certificación, la validación de certificados del servidor se deshabilita y el dispositivo intentará autenticarse a sí mismo independientemente de la red a la que esté conectado.

Si se usa un certificado, en la implementación de Axis, el dispositivo y el servidor de autentificación se autentican ellos mismos con certificados digitales utilizando EAP-TLS (protocolo de autenticación extensible - seguridad de la capa de transporte).

Para permitir que el dispositivo acceda a una red protegida mediante certificados, debe instalar un certificado de cliente firmado en el dispositivo.

Authentication method (Método de autentificación): Seleccione un tipo de EAP utilizado para la autentificación.

Client certificate (Certificado del cliente): Seleccione un certificado de cliente para usar IEEE 802.1x. El servidor de autentificación utiliza el certificado para validar la identidad del cliente.

CA Certificates (Certificados CA): Seleccione certificados CA para validar la identidad del servidor de autentificación. Si no se selecciona ningún certificado, el dispositivo intentará autenticarse a sí mismo, independientemente de la red a la que esté conectado.

EAP identity (Identidad EAP): Introduzca la identidad del usuario asociada con el certificado de cliente.

EAPOL version (Versión EAPOL): Seleccione la versión EAPOL que se utiliza en el switch de red.

Use IEEE 802.1x (Utilizar IEEE 802.1x): Seleccione para utilizar el protocolo IEEE 802.1x.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1x PEAP-MSCHAPv2** como método de autentificación:

- **Contraseña**: Escriba la contraseña para la identidad de su usuario.
- **Versión de Peap**: Seleccione la versión de Peap que se utiliza en el switch de red.
- **Label (Etiqueta)**: Seleccione 1 para usar el cifrado EAP del cliente; seleccione 2 para usar el cifrado PEAP del cliente. Seleccione la etiqueta que utiliza el switch de red cuando utilice la versión 1 de Peap.

Estos ajustes solo están disponibles si utiliza **IEEE 802.1ae MACsec (CAK estática/clave precompartida)** como método de autenticación:

- **Nombre de clave de asociación de conectividad de acuerdo de claves:** Introduzca el nombre de la asociación de conectividad (CKN). Debe tener de 2 a 64 caracteres hexadecimales (divisibles por 2). La CKN debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.
- **Clave de asociación de conectividad de acuerdo de claves**: Introduzca la clave de la asociación de conectividad (CAK). Debe tener una longitud de 32 o 64 caracteres hexadecimales. La CAK debe configurarse manualmente en la asociación de conectividad y debe coincidir con los dos extremos del enlace para activar inicialmente MACsec.

Evitar ataques de fuerza bruta

Blocking (Bloqueo): Active esta función para bloquear ataques de fuerza bruta. Un ataque de fuerza utiliza un sistema de ensayo y error para descubrir información de inicio de sesión o claves de cifrado.

Blocking period (Período de bloqueo): Introduzca el número de segundos para bloquear un ataque de fuerza bruta.

Blocking conditions (Condiciones de bloqueo): Introduzca el número de fallos de autenticación permitidos por segundo antes de que se inicie el bloqueo. Puede definir el número de fallos permitidos tanto a nivel de página como de dispositivo.

Firewall

Firewall: Encender para activar el firewall.

Política predeterminada: Seleccione cómo desea que el firewall gestione las solicitudes de conexión no cubiertas por las reglas.

- **ACCEPT (Aceptar):** Permite todas las conexiones al dispositivo. Esta opción está establecida de forma predeterminada.
- **DROP (Soltar):** Bloquea todas las conexiones al dispositivo.

Para realizar excepciones a la política predeterminada, puede crear reglas que permitan o bloqueen las conexiones al dispositivo desde direcciones, protocolos y puertos específicos.

+ New rule (Nueva regla): Haga clic para crear una regla.

Rule type (Tipo de regla):

- **FILTER (FILTRO)**: Seleccione esta opción para permitir o bloquear conexiones de dispositivos que coincidan con los criterios definidos en la regla.
  - **Policy (Directiva)**: Seleccione **Accept (Aceptar)** o **Drop (Soltar)** para la regla del firewall.
  - **IP range (Intervalo IP)**: Seleccione para especificar el rango de direcciones que desee permitir o bloquear. Utilice IPv4/IPv6 en **Start (Inicio)** y **End (Fin)**.
  - **IP address (Dirección IP)**: Introduzca la dirección que desee permitir o bloquear. Use el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo)**: Seleccione el protocolo de red (TCP, UDP o Ambos) que desee permitir o bloquear. Si selecciona un protocolo, también deberá especificar un puerto.
  - **MAC**: Introduzca la dirección MAC del dispositivo que desee permitir o bloquear.
  - **Port range (Intervalo de puertos)**: Seleccione esta opción para especificar el rango de puertos que desee permitir o bloquear. Añádalos en **Start (Inicio)** y **End (Fin)**.
  - **Port (Puerto)**: Introduzca el número de puerto que desee permitir o bloquear. Los números de puerto deben situarse estar entre 1 y 65535.
  - **Traffic type (Tipo de tráfico)**: Seleccione el tipo de tráfico que desee permitir o bloquear.
    - **UNICAST** (Unidifusión): Tráfico de un único emisor a un único destinatario.
    - **BROADCAST (TRANSMISIÓN)**: Tráfico de un único emisor a todos los dispositivos de la red.
    - **MULTICAST**: Tráfico de uno o varios emisores a uno o más destinatarios.
- **LIMIT (Límite)**: Seleccione esta opción para aceptar conexiones de dispositivos que coincidan con los criterios definidos en la regla, pero aplique límites para reducir el tráfico excesivo.
  - **IP range (Intervalo IP)**: Seleccione para especificar el rango de direcciones que desee permitir o bloquear. Utilice IPv4/IPv6 en **Start (Inicio)** y **End (Fin)**.
  - **IP address (Dirección IP)**: Introduzca la dirección que desee permitir o bloquear. Use el formato IPv4/IPv6 o CIDR.
  - **Protocol (Protocolo)**: Seleccione el protocolo de red (TCP, UDP o Ambos) que desee permitir o bloquear. Si selecciona un protocolo, también deberá especificar un puerto.
  - **MAC**: Introduzca la dirección MAC del dispositivo que desee permitir o bloquear.
  - **Port range (Intervalo de puertos)**: Seleccione esta opción para especificar el rango de puertos que desee permitir o bloquear. Añádalos en **Start (Inicio)** y **End (Fin)**.
  - **Port (Puerto)**: Introduzca el número de puerto que desee permitir o bloquear. Los números de puerto deben situarse estar entre 1 y 65535.
  - **Unit (Unidad)**: Seleccione el tipo de conexiones que desee permitir o bloquear.
  - **Period (Periodo)**: Seleccione el periodo de tiempo relacionado con **Amount (Cantidad)**.
  - **Amount (Cantidad)**: Determine el número máximo de veces que se permite que un dispositivo se conecte dentro del **Period (Periodo)**. La cantidad máxima es 65535.

- **Burst (Ráfaga)**: Introduzca el número de conexiones que pueden superar la **Amount (Cantidad)** establecida una vez durante el **Period (Periodo)** establecido. Una vez alcanzado el número, solo se permitirá la cantidad determinada durante el periodo establecido.
- **Traffic type (Tipo de tráfico)**: Seleccione el tipo de tráfico que desee permitir o bloquear.
  - **UNICAST** (Unidifusión): Tráfico de un único emisor a un único destinatario.
  - **BROADCAST (TRANSMISIÓN)**: Tráfico de un único emisor a todos los dispositivos de la red.
  - **MULTICAST**: Tráfico de uno o varios emisores a uno o más destinatarios.

Test rules (Prueba de reglas): Haga clic para probar las reglas que haya definido.

- **Test time in seconds (Tiempo de prueba en segundos)**: Defina un límite de tiempo para probar las reglas.
- **Roll back (Restaurar)**: Haga clic para restablecer el firewall a su estado anterior, antes de haber probado las reglas.
- **Apply rules (Aplicar reglas)**: Haga clic para activar las reglas sin probarlas. No le recomendamos esta opción.

Certificado de AXIS OS con firma personalizada

Para instalar en el dispositivo software de prueba u otro software personalizado de Axis, necesita un certificado de AXIS OS firmado personalizado. El certificado verifica que el software ha sido aprobado por el propietario del dispositivo y por Axis. El software solo puede ejecutarse en un dispositivo específico identificado por su número de serie e ID de chip, que son únicos. Solo Axis puede crear certificados de AXIS OS firmados personalizados, ya que Axis posee la clave para firmarlos.

Install (Instalar): Haga clic para instalar el certificado. El certificado se debe instalar antes que el software.

El menú contextual contiene:

- **Delete certificate (Eliminar certificado)**: Se elimina el certificado.

Cuentas

Cuentas de dispositivo

Cuentas

Add account (Añadir cuenta): Haga clic para agregar una nueva cuenta. Puede agregar hasta 100 cuentas.

Cuenta: introduzca un nombre de cuenta único.

Nueva contraseña: introduzca una contraseña para la cuenta. Las contraseñas deben tener entre 1 y 64 caracteres. La contraseña solo admite caracteres ASCII imprimibles (códigos de 32 a 126), por ejemplo, letras, números, signos de puntuación y algunos símbolos.

Repetir contraseña: Introduzca la misma contraseña de nuevo.

Privilegios:

- **Administrador**: Tiene acceso completo a todos los ajustes. Los administradores también pueden agregar, actualizar y eliminar otras cuentas.
- **Operator (Operador)**: Tiene acceso a todos los ajustes excepto:
  - Todos los ajustes del **sistema**.
- **Viewer (Visualizador)**: No tiene acceso para cambiar ajustes.

El menú contextual contiene:

Actualizar cuenta: Editar las propiedades de la cuenta.

Eliminar cuenta: Elimine la cuenta. No puede eliminar la cuenta de root.

MQTT

MQTT (Message Queuing Telemetry Transport) es un protocolo de mensajería estándar para Internet of things (IoT). Se diseñó para simplificar la integración del IoT y se utiliza en una amplia variedad de sectores para conectar dispositivos remotos con una huella de código pequeña y un ancho de banda de red mínimo. El cliente MQTT del software de dispositivos de Axis puede simplificar la integración de los datos y eventos producidos en el dispositivo con sistemas que no sean software de gestión de vídeo (VMS).

Configure el dispositivo como cliente MQTT. La comunicación MQTT se basa en dos entidades, los clientes y el intermediario. Los clientes pueden enviar y recibir mensajes. El intermediario es responsable de dirigir los mensajes entre los clientes.

Puede obtener más información sobre MQTT en la *base de conocimiento de AXIS OS*.

ALPN

ALPN es una extensión de TLS/SSL que permite seleccionar un protocolo de aplicación durante la fase de enlace de la conexión entre el cliente y el servidor. Se utiliza para habilitar el tráfico MQTT a través del mismo puerto que se utiliza para otros protocolos, como HTTP. En algunos casos, es posible que no haya un puerto dedicado abierto para la comunicación MQTT. Una solución en tales casos es utilizar ALPN para negociar el uso de MQTT como protocolo de aplicación en un puerto estándar, permitido por los cortafuegos.

Cliente MQTT

Conectar: Active o desactive el cliente MQTT.

Estado: Muestra el estado actual del cliente MQTT.

Broker

Host: introduzca el nombre de host o la dirección IP del servidor MQTT.

Protocol (Protocolo): Seleccione el protocolo que desee utilizar.

Port (Puerto): Introduzca el número de puerto.

- 1883 es el valor predeterminado de **MQTT over TCP (MQTT a través de TCP)**
- 8883 es el valor predeterminado de **MQTT a través de SSL**
- 80 es el valor predeterminado de **MQTT a través de WebSocket**
- 443 es el valor predeterminado de **MQTT a través de WebSocket Secure**

Protocol ALPN: Introduzca el nombre del protocolo ALPN proporcionado por su proveedor de MQTT. Esto solo se aplica con MQTT a través de SSL y MQTT a través de WebSocket Secure.

Nombre de usuario: Introduzca el nombre de cliente que utilizará la cámara para acceder al servidor.

Contraseña: Introduzca una contraseña para el nombre de usuario.

Client ID (ID de cliente): Introduzca un identificador de cliente. El identificador de cliente se envía al servidor cuando el cliente se conecta a él.

Clean session (Limpiar sesión): Controla el comportamiento en el momento de la conexión y la desconexión. Si se selecciona, la información de estado se descarta al conectar y desconectar.

Proxy HTTP: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTP.

Proxy HTTPS: Una URL con una longitud máxima de 255 bytes. Puede dejar el campo vacío si no desea utilizar un proxy HTTPS.

Keep alive interval (Intervalo de Keep Alive): Habilita al cliente para detectar si el servidor ya no está disponible sin tener que esperar a que se agote el tiempo de espera de TCP/IP.

Timeout (Tiempo de espera): El intervalo de tiempo está en segundos para permitir que se complete la conexión. Valor predeterminado: 60

Device topic prefix (Prefijo de tema del dispositivo): se utiliza en los valores por defecto del tema en el mensaje de conexión, en el mensaje LWT de la pestaña **MQTT client (Cliente MQTT)** y, en las condiciones de publicación de la pestaña **MQTT publication (Publicación MQTT)** ".

Reconnect automatically (Volver a conectar automáticamente): especifica si el cliente debe volver a conectarse automáticamente tras una desconexión.

Mensaje de conexión

Especifica si se debe enviar un mensaje cuando se establece una conexión.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Mensaje de testamento y últimas voluntades

El testamento y últimas voluntades (LWT) permite a un cliente proporcionar un testimonio junto con sus credenciales al conectar con el intermediario. Si el cliente se desconecta de forma no voluntaria (quizá porque no dispone de fuente de alimentación), puede permitir que el intermediario entregue un mensaje a otros clientes. Este mensaje de LWT tiene el mismo formato que un mensaje normal y se enruta a través de la misma mecánica.

Enviar mensaje: Active esta función para enviar mensajes.

Usar predeterminado: Desactive esta opción para introducir su propio mensaje predeterminado.

Topic (Tema): Introduzca el tema para el mensaje predeterminado.

Payload (Carga): Introduzca el contenido para el mensaje predeterminado.

Retain (Retener): Seleccione esta opción para mantener el estado del cliente en este **Tema**

QoS: Cambie la capa de QoS para el flujo de paquetes.

Publicación MQTT

Usar prefijo de tema predeterminado: Seleccione esta opción para utilizar el prefijo de tema predeterminado, que se define en el prefijo de tema del dispositivo en la pestaña **Cliente MQTT**.

Include condition (Incluir condición): Seleccione esta opción para incluir el tema que describe la condición en el tema de MQTT.

Include namespaces (Incluir espacios de nombres): Seleccione esta opción para incluir los espacios de nombres de los temas ONVIF en el tema MQTT.

Include serial number (Incluir número de serie): seleccione esta opción para incluir el número de serie del dispositivo en la carga útil de MQTT.

Add condition (Añadir condición): Haga clic para agregar una condición.

Retain (Retener): define qué mensajes MQTT se envían como retenidos.

- **None (Ninguno)**: envíe todos los mensajes como no retenidos.
- **Property (Propiedad)**: envíe únicamente mensajes de estado como retenidos.
- **All (Todo)**: Envíe mensajes con estado y sin estado como retenidos.

QoS: Seleccione el nivel deseado para la publicación de MQTT.

Suscripciones MQTT

Add subscription (Añadir suscripción): Haga clic para agregar una nueva suscripción MQTT.

Filtro de suscripción: Introduzca el tema de MQTT al que desea suscribirse.

Nota

Si opta por editar el filtro de suscripción, asegúrese de actualizar los eventos conectados.

Usar prefijo de tema del dispositivo: Agregue el filtro de suscripción como prefijo al tema de MQTT.

Tipo de suscripción:

- **Sin estado**: Seleccione esta opción para convertir mensajes MQTT en mensajes sin estado.
- **Con estado**: Seleccione esta opción para convertir los mensajes MQTT en una condición. El contenido se utiliza como estado.

QoS: Seleccione el nivel deseado para la suscripción a MQTT.

Accesorios

Puertos de E/S

Use la entrada digital para conectar seguridad positiva que pueda alternar entre circuitos abiertos y cerrados, por ejemplo, sensores PIR, contactos de puertas o ventanas y detectores de cristales rotos.

Use la salida digital para establecer conexión con dispositivos externos, como relés y LED. Puede activar los dispositivos conectados a través de la interfaz de programación de aplicaciones VAPIX® o la interfaz web.

Puerto

Name (Nombre): Edite el texto para cambiar el nombre del puerto.

Direction (Dirección):  indica que el puerto es un puerto de entrada.  indica que es un puerto de salida. Si el puerto es configurable, puede hacer clic en los iconos para cambiar entre entrada y salida.

Normal state (Estado normal): Haga clic en  para circuito abierto y en  para circuito cerrado.

Current State (Estado actual): muestra el estado actual del puerto. La entrada o salida se activa cuando el estado actual difiere del estado normal. Una entrada del dispositivo tiene el circuito abierto cuando está desconectado o cuando hay una tensión superior a 1 V CC.

Nota

Durante el reinicio, se abre el circuito de salida. Cuando termina el reinicio, el circuito vuelve a la posición normal. Si modifica algún ajuste de esta página, los circuitos de salida recuperan las posiciones normales, con independencia de los activadores activos.

Supervised (Supervisado): Active esta opción para que sea posible detectar y activar acciones si alguien manipula la conexión con dispositivos de E/S digital. Además de detectar si una entrada está abierta o cerrada, también puede detectar si alguien la ha manipulado (mediante un corte o cortocircuito). La supervisión de la conexión requiere hardware adicional (resistencias de final de línea) en el bucle de E/S externa.

Registros

Informes y registros

Informes

- **Ver informe del servidor del dispositivo**: Consulte información acerca del estado del producto en una ventana emergente. El registro de acceso se incluye automáticamente en el informe del servidor.
- **Download the device server report (Descargar informe del servidor del dispositivo)**: Crea un archivo .zip que incluye un archivo de texto en formato UTF–8 con un informe completo del servidor. Para incluir la instantánea de la imagen actualmente en visualización en directo, seleccione **Include image (Incluir imagen)**. Incluya siempre el archivo. zip del informe del servidor si necesita contactar con el servicio de asistencia.
- **Download the crash report (Descargar informe de fallos)**: Descargar un archivo con la información detallada acerca del estado del servidor. El informe de fallos incluye información ya presente en el informe del servidor, además de información detallada acerca de la corrección de fallos. Este informe puede incluir información confidencial, como trazas de red. Puede tardar varios minutos en generarse.

Registros

- **View the system log (Ver registro del sistema)**: Haga clic para consultar información acerca de eventos del sistema como inicio de dispositivos, advertencias y mensajes críticos.
- **View the access log (Ver registro de acceso)**: Haga clic para ver todos los intentos incorrectos de acceso al dispositivo, por ejemplo, si se utiliza una contraseña de inicio de sesión incorrecta.
- **View the audit log (Ver registro de auditoría)**: Haga clic para mostrar información sobre las actividades del usuario y del sistema, por ejemplo, autentificaciones y configuraciones correctas o fallidas.

Rastreo de red

Importante

Un archivo de rastreo de red puede contener información confidencial, por ejemplo, certificados o contraseñas.

Un archivo de rastreo de red puede ayudar a solucionar problemas mediante la grabación de la actividad en la red.

Trace time (Tiempo de rastreo): Seleccione la duración del rastreo en segundos o minutos y haga clic en **Descargar**.

Registro de sistema remoto

Syslog es un estándar de registro de mensajes. Permite que el software que genera los mensajes, el sistema que los almacena y el software que los notifica y analiza sean independientes. Cada mensaje se etiqueta con un código de instalación, que indica el tipo de software que genera el mensaje y tiene un nivel de gravedad.

 **Server (Servidor)**: Haga clic para agregar un nuevo servidor.

Host: introduzca el nombre de host o la dirección IP del servidor.

Format (Formato): Seleccione el formato de mensaje de syslog que quiera utilizar.

- Axis
- RFC 3164
- RFC 5424

Protocol (Protocolo): Seleccione el protocolo que desee utilizar:

- UDP (el puerto predeterminado es 514).
- TCP (el puerto predeterminado es 601).
- TLS (el puerto predeterminado es 6514).

Port (Puerto): Modifique el número de puerto para usar otro puerto.

Severity (Gravedad): Seleccione los mensajes que se enviarán cuando se activen.

Tipo: Seleccione el tipo de registros que desea enviar.

Test server setup (Probar configuración del servidor): Envíe un mensaje de prueba a todos los servidores antes de guardar la configuración.

CA certificate set (Conjunto de certificados de CA): Consulte los ajustes actuales o añada un certificado.

Maintenance (Mantenimiento):

Restart (Reiniciar): Reiniciar el dispositivo. No afectará a la configuración actual. Las aplicaciones en ejecución se reinician automáticamente.

Restore (Restaurar): Casi todos los ajustes vuelven a los valores predeterminados de fábrica. Después deberás reconfigurar el dispositivo y las aplicaciones, reinstalar las que no vinieran preinstaladas y volver a crear los eventos y preajustes.

Importante

Los únicos ajustes que se guardan después de una restauración son:

- Protocolo de arranque (DHCP o estático)
- Dirección IP estática
- Router predeterminado
- Máscara de subred
- Configuración 802.1X
- Configuración de O3C
- Dirección IP del servidor DNS

Factory default (Predeterminado de fábrica): Todos los ajustes vuelven a los valores predeterminados de fábrica. Después, es necesario restablecer la dirección IP para poder acceder al dispositivo.

Nota

Todo el software de los dispositivos AXIS está firmado digitalmente para garantizar que solo se instala software verificado. Esto aumenta todavía más el nivel mínimo general de ciberseguridad de los dispositivo de Axis. Para obtener más información, consulte el documento técnico "Axis Edge Vault" en *axis.com*.

Actualización de AXIS OS: Se actualiza a una nueva versión de AXIS OS. Las nuevas versiones pueden contener mejoras de funciones, correcciones de errores y características totalmente nuevas. Le recomendamos que utilice siempre la versión de AXIS OS más reciente. Para descargar la última versión, vaya a *axis.com/support*.

Al actualizar, puede elegir entre tres opciones:

- **Standard upgrade (Actualización estándar)**: Se actualice a la nueva versión de AXIS OS.
- **Factory default (Predeterminado de fábrica)**: Se actualiza y todos los ajustes vuelven a los valores predeterminados de fábrica. Si elige esta opción, no podrá volver a la versión de AXIS OS anterior después de la actualización.
- **Automatic rollback (Restauración automática)**: Se actualiza y debe confirmar la actualización en el plazo establecido. Si no confirma la actualización, el dispositivo vuelve a la versión de AXIS OS anterior.

Restaurar AXIS OS: Se vuelve a la versión anterior de AXIS OS instalado.

T10125657_es

2026-09 (M15.3)

© 2018 – 2026 Axis Communications AB